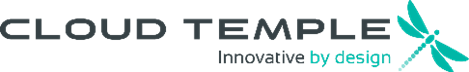
IaaS Service Agreement



Cloud Temple Logo

# 1. **IaaS SERVICES AGREEMENT**

| **Recipients:** | **CLIENT** |
| --- | --- |
| **Document Reference** | CT.AM.JUR.ANX - 20240403\_v2.0.docx\_Day DD YYYY |
| **Your Contacts** | *First Name* *Last Name* |
|  | Account Manager |
|  | e-mail: *first.name*@cloud-temple.com |
| **Last Update Date** | April 3, 2024 |
| **Contractual Validation Date** | Day DD YYYY |

| **Version** | **Date** | **Action** | **Author** |
| --- | --- | --- | --- |
| v0.1 | June 7, 2022 | Initial Drafting | Lorena ALCALDE |
| v0.2 | Sept 14, 2022 | Enrichment | Lorena ALCALDE |
| v1.0 | Dec 30, 2022 | Integration of Indicators | Lorena ALCALDE |
| v1.1 | Jan 23, 2023 | Footer Modification | Lorena ALCALDE |
| v1.2 | May 22, 2023 | Enrichment | Lorena ALCALDE |
| v1.3 | June 29, 2023 | Enrichment | Lorena ALCALDE |
| v1.4 | Nov 6, 2023 | Modification of Capital and Enrichment | Lorena ALCALDE |
| v1.5 | Nov 30, 2023 | Enrichment | Lorena ALCALDE |
| v1.6 | Mar 21, 2024 | Enrichment | Lorena ALCALDE |
| v2.0 | Mar 29, 2024 | Compliance Adjustments SNC | Nicolas ABRIOUX |
| v2.0 | April 3, 2024 | Publication | Lorena ALCALDE |

# 2. **TABLE OF CONTENTS**

* [1. **IaaS SERVICES AGREEMENT**](#X6e12c00f7864180c8b65bed452c693d98eb38cd)
* [2. **TABLE OF CONTENTS**](#X6b2593602a0c62157c0c7b32214e273425badb5)
* [3. Preliminary and Glossary](#Xf612288235422c94abee43ac74cdffdb32f3070)
  + [3.1. Preliminary](#X0861222e820450c490ca907d976d4d876859686)
  + [3.2 Glossary](#Xbd6ce1e9ddf2e6b4ed68b43cca36e39b1dff4f8)
* [4. Acronyms](#X63082f47fbddb08c599db439657feb8fbdb7b4c)
* [5. Purpose of the present Service Convention](#Xbf426983f1396be94dab6737a400d1241251527)
* [6. Audit](#X910e2801262de94af715f54b8fb509cc70cc79a)
* [7. Service Description](#X701ae114948e6c3c2ae1cbf85ab3e7bf1880db7)
  + [7.1. Shared Responsibility Model](#X4a98f4c089eb84711ad4fcecdc4c7a8c3b033c9)
  + [7.2. Detailed Presentation of the Service Scope](#Xe4dff9194e06af051c42f5767ecc4a719eaba71)
    - [7.2.1. Datacenter Infrastructures](#X02b6ed0df8b3694b272e6917b4853b73c3a948c)
    - [7.2.2. Software infrastructure for Service management](#X1aab31ed1fac34aad3b1f4bb31d8482b9443c36)
    - [7.2.3. Computing Infrastructures](#X2a77c168d5abc99557aec5f49f7672b54c7b789)
    - [7.2.4. Storage Infrastructure](#Xb02786eb8f8bd88452ea9d047200b5d55601d0d)
    - [7.2.5. Global Network Infrastructure](#Xbe28a1904b65f69820d471cda7494866dc1453a)
    - [7.2.6. Backup Infrastructure](#X964f2fd6ec5cc040407ceb29c331cdfc91a064a)
    - [7.2.7. Implementation of Disaster Recovery or Business Continuity Solutions](#X46342410f6bb16be35c09e31b55936206078422)
  + [7.3. Limitations of Services in the Qualified IaaS Model](#Xfc62b9ce9407e2feea20a9138d78902765217d8)
    - [7.3.1. Managed Services in RUN](#X0b812967fb989ab1bada217b8566d278dd5d2a7)
    - [7.3.2. Disaster Recovery Configuration](#X0c63f3a7ed22b82c174a5da627b69a71fa62fae)
    - [7.3.3. Backup Configuration](#X34c0a9ad2233ede3ecab52b69189ddb0d3f0503)
  + [7.4. Implementation of the service](#Xb287de9901d5c07ddff055f449307df664a91db)
    - [7.4.1. Technical Prerequisites](#X60d9652fab274d39d04bd36d22bf4c454b39299)
  + [7.5. Service Localization in France](#X4063c3c418d0448a51a21d4b38546197e079a52)
    - [7.5.1. Location of Datacenters Hosting the Service](#Xe2604f24f7a41fe808134d5ce4a503036c1cacb)
    - [7.5.2. Location of Cloud Temple Agencies Operating the Service](#Xf5d7c9302725838f5c14e51905ae7852efcdd1b)
  + [7.6. Support](#X451baaab9b4764d97da95395b7e24265143a283)
    - [7.6.1. Nature of Support Accompanying the Service](#X3d8427579315d204d1739c824f9b51c0e77b6ba)
    - [7.6.2. Requesting technical support service](#Xcade472761b201f4e24c0b87f4deec763b07dce)
    - [7.6.3. Incident Management Process](#X9bcf8c4cdcd19d01f19ce35ee3d62d9884f2ea1)
    - [7.6.4. Prioritization Process of Treatments](#X0b7d7da20c17023e4d43e00d866caeac9526733)
    - [7.6.5. Language and localization of the support service](#X7ea3826319d55143a85d037351863bc15c408c5)
* [8. Commitments and Service Levels](#X1c89a72470893337f86f8d6da4eaaed1e31a103)
  + [8.1. Service Infrastructure Availability Commitments](#Xd9dcebf55cded024008c2c577d0e093783410e8)
  + [8.2. Availability commitment of the SPONSOR interface](#X516b6bad93a618ec8836233ff156c4aa43e0ed3)
  + [8.3. Availability Commitment of Support](#X2d004efb0877159af83124c4ebdeec9b424f3b8)
  + [8.4. Commitment to S3 object storage availability](#Xaa94a2a178892dceb39022a9441328843a34994)
  + [8.5. Clarification regarding the backup commitment](#X5d597e12b8c3692cefaefccdca2f34d99ec680c)
* [9. Organization of the Contractual Relationship](#X588e6b4c8468013ccc6e54510dd3a263d8727b6)
  + [9.1. Provider’s Responsibilities](#X644463cb6485f7959caeae4688c6cc688395f9a)
  + [9.2. Limitation of the Service Provider’s Liabilities](#X26057e298607630f9964707393bf7bd0ac59509)
  + [9.3. Access Limitation](#X04d8a2ca99269a299efe766dc983f39ed99a75f)
  + [9.4. Responsibilities of Third Parties Participating in the Provision of the Secure Temple Service](#Xc4b23c2f8d579d563eab7ceb7bdffeeb3276802)
  + [9.5. Responsibilities and obligations of the SPONSOR](#Xc748d95977daf06b0d0e46702a9ecf50f3ca0e8)
  + [9.6. Rights of the CLIENT](#X37751fa5e814593cadebcf668dba30f6dc41e00)
  + [9.7. Data Deletion at the End of the Contract](#X451d0e06737540a859fb31f6450e3946e3ec09a)
* [10. Life Cycle of the Current Service Agreement](#X2a3397bca43c8cfe74edb2f6109d0fe975f3d6e)
  + [10.1. Entry into Effect of the Service Agreement](#Xa1e347ff54237d0a2690725e905735df9fb9e01)
  + [10.2. Amendments to the Service Agreement](#X31269eaa6404af7ba2257a880c115c88cef401c)
    - [10.2.1. Evolutions Triggered by the SPONSOR](#X49a3e7a6eb7e4814f51de43353868f21240dc7f)
    - [10.2.2. Amendments Initiated by the Service Provider](#Xbd2dc631b9fe45871bda5387c572d688c13d362)
  + [10.3. Reversibility](#Xecde706c6406b34c8efdf272698d0631b5e9c5f)
* [11. Availability, Continuity, and Service Restoration](#X58b383e2614dc798f856a41905cc32ad106b2b1)
  + [11.1. Incident and Interruption Management](#X98baf3a4009a822296df53f4bf062054c2843fd)
    - [11.1.1. Incidents](#X648046c564ac1cd52bebb02b256b193a3da4d74)
      * [11.1.1.1. Types of Incidents Addressed Under this Service Level Agreement](#X353772e4dd0ab1750c92f0a66326d633b890956)
      * [11.1.1.2. Incident Management](#Xd5cfa2f2d2890259872da41d81814c298443136)
      * [11.1.1.3. Security Incident Notification Level](#X6ab67dd20cec6628f87440cfb1e200c9ad91550)
  + [11.2 Service Maintenance](#X0c68675836078f8b8ab76887a2c3f3216fb2f77)
    - [11.2.1. Nature of Maintenance](#Xbfd135e29c67f5e12ddc792f7a150d24910a481)
    - [11.2.2 Remote Access by Cloud Temple to the SPONSOR’s Scope](#X48b64b7037db3c18c2eccb771cb5325638a2ee0)
    - [11.2.3. Remote Third-Party Access Participating in the Service Provision within the COMMANDITAIRE’s Scope](#Xda1b309a8cc7bfe21c153c7c0190f3718119f53)
* [12. Procedure for Data Deletion at the End of the Contract](#X9579f2c80b47ab1ef3d1e330147b2cae904e3ca)
* [13. Applicable Law](#X2aeb29653e9d8a9d9ca459b3352c7c2213d84e0)
  + [13.1. In General](#Xdbdfc7bdc3699100cdfa80457c495c9e2f03280)
  + [13.2. Compliance with Applicable Laws and Regulations](#Xf31e553dc0f62fefd647dbb143cdf0b63cb1176)
  + [13.3. GDPR](#X7b71b74ecdc4639f1cdd9f5882fc9e82eee0b01)
  + [13.4. Protection Concerning Non-European Law](#Xa664431679293fec2b6a3fa4bcaac1c7d078962)
* [14. SIGNATURES](#X7ad993788a708b47017c27c9d96178e8795e44f)

# 3. Preliminary and Glossary

## 3.1. Preliminary

This document formalizes the Service Agreement associated with the IaaS service qualified as SecNumCloud under the name “Secure Temple.”

“This Service Agreement supplements and complements the General Terms and Conditions of Sale and Use of the Provider. It is understood that the contractual documents are to be interpreted consistently with one another. In the event of a contradiction or divergence between the terms of the contractual documents, the documents will prevail over each other in the following order:

1. General Terms and Conditions of Sale and Use (GTC)
2. SecNumCloud IaaS Service Agreement
3. SecNumCloud PaaS Service Agreement
4. Specific Individual Agreement
5. Security Assurance Plan (SAP)
6. Specific Terms of Use (STU)

## 3.2 Glossary

In the present Service Agreement, the **SPONSOR**, the **Provider**, and the **Parties** are identified in the Contract to which this Service Agreement is annexed.

The expressions used herein shall be interpreted in accordance with the definitions assigned to them below:

* **Change**: Any addition, modification, or deletion affecting the Service, which has been authorized, planned, or undertaken.
* **Standard Change**: A change subject to a procedure, the terms of implementation and impacts (including financial) of which are known and accepted in advance by the Parties. It is then integrated into the standard change catalog and may have an SLA (Service Level Agreement) and an MTTR (Mean Time To Repair).
* **Contract**: Refers to the contract subscribed by the SPONSOR with the Provider to enable the SPONSOR to benefit from the Service, to which this Service Agreement is annexed.
* **Service Agreement**: This document, established within the framework of a specific contract or the General Terms and Conditions of Sale and Use (CGVU), and in compliance with the requirements of the SecNumCloud Framework.
* **Service Request**: A request from the SPONSOR to the Provider within the scope of the Service, covering operations not executable by the SPONSOR from the SPONSOR interface and support requests within the Service. Service requests are limited to those provided under the Contract or this Service Agreement.
* **Availability**: The ability to ensure the availability and maintenance of optimal performance of the Service, in accordance with the criteria and commitments defined in the Service Level Agreements (SLAs).
* **Technical Data**: Includes all data manipulated to deliver the Service, notably including the identity of the beneficiary and the technical infrastructure administrators, technical infrastructure logs, access configuration, directory, certificates, etc.
* **Event**: An “event” is any detectable or identifiable occurrence that may be significant for the management of the Service.
* **Hypervisor**: Operating system allowing the execution of virtual machines on a computing blade.
* **Incident**: Any unexpected event that disrupts the normal function of the Service or compromises the security of the data.
* **Security Incident**: Any event within the scope of the Service:
  + Of an intentionally malevolent nature;
  + Of an accidental nature affecting the integrity, confidentiality, or traceability of the Service or the SPONSOR’s data;
  + Affecting the existing security measures. Availability breaches of non-malicious origin are not considered as Security Incidents (hardware failure, bug, malfunction, natural disaster, etc.).
* **SPONSOR Interface**: The Service administration interface provided to the SPONSOR by the Provider, comprising a web administration console and an API.
* **Deployment**: The administration action(s) to realize the Change once it is approved (the change, in the ITIL sense, only concerning the management of change and not its actual implementation).
* **Problem**: The cause of one or more recurrent Incidents, causal of a potential Incident (risk situation).
* **Region**: Refers to a geographically defined set of cloud availability zones, providing network, computation, and storage services to optimize latency, performance, and local regulatory compliance.
* **Service**: Refers to the IaaS service qualified as SecNumCloud “Secure Temple”, delivered to the SPONSOR by the Provider from the technical infrastructures maintained by the Provider, as described in the “Description of Service” section of this Service Agreement.
* **Secure Temple**: Refers to the IaaS service qualified as SecNumCloud, offered by the company Cloud Temple, as defined in the certificate available on the ANSSI website and provided in the annex of this Service Agreement.
* **Disaster**: Refers to a serious event of natural or human origin, whether accidental or intentional, causing significant loss and damage to the affected Party.
* **Monitoring**: Surveillance of an Information System or a Service, involving the collection of various data such as measurements and alarms. This activity is limited to observation and tracking, without directly intervening on the monitored elements, a prerogative belonging to Administration operations.
* **Tenant**: An isolated instance reserved for a user or group of users, sharing a common infrastructure while maintaining the independence and security of data and applications.
* **Availability Zone (AZ)**: A specific and isolated section of the cloud computing infrastructure, designed to ensure the high availability and resilience of services by geographic distribution of resources.

# 4. Acronyms

| **Acronym** | **Definition** |
| --- | --- |
| **CAB** | Change Advisory Board – Advisory Committee on Changes |
| **CMDB** | Configuration Management Database – Database for Configuration Management |
| **COPIL** | Steering Committee |
| **COSTRAT** | Strategic Committee |
| **COPROJ** | Project Committee |
| **DB** | Database |
| **DRP** | Disaster Recovery Plan |
| **GTE** | Guarantee of Escalation Time |
| **GTI** | Guarantee of Intervention Time |
| **GTR** | Guarantee of Resolution Time |
| **ITIL** | Information Technology Infrastructure Library - Best practices for IT management |
| **IaaS** | Infrastructure as a Service |
| **MCO** | Operational Condition Maintenance |
| **MOA** | Contracting Authority |
| **MOE** | Prime Contractor |
| **MSP** | Managed Services Provider |
| **OS** | Operating System |
| **PAQ** | Quality Assurance Plan |
| **PaaS** | Platform as a Service |
| **PAS** | Security Assurance Plan |
| **PASSI** | Security Systems Information Audit Service Provider |
| **RFC** | Request For Change – Change Request |
| **RGPD** | General Data Protection Regulation |
| **RPO** | Recovery Point Objective – Freshness of data restored in the event of a Disaster |
| **RTO** | Recovery Time Objective – Service restoration time in the event of a Disaster |
| **SDM** | Service Delivery Manager |
| **SLA** | Service Level Agreement – Agreement on service levels |
| **SNC** | SecNumCloud |
| **SOC** | Security Operation Center |
| **TMA** | Application Maintenance Outsourcing |
| **UO** | Work Unit |
| **VABE** | Aptitude Validation for Good Operability |
| **VABF** | Aptitude Validation for Good Functioning |
| **VM** | Virtual Machine |
| **VSR** | Regular Service Validation |

# 5. Purpose of the present Service Convention

The present Service Agreement establishes the terms and conditions under which the Provider undertakes to deliver the Service to the SPONSOR. Its purpose is to:

* Specify the performance requirements expected by the SPONSOR in terms of functionality and reliability of the Service;
* State the Provider’s obligations to meet the agreed service levels;
* Identify the regulatory standards specifically applicable to the Service provided;
* Ensure uniformity and integrity in the assessment of Service quality;
* Guarantee the excellence of the provided services, evaluated using quantitative performance indicators.

It is stipulated that, in the event that the Provider is stripped of its SecNumCloud qualification, the Contract may be terminated by right, without incurring penalties, by the SPONSOR. In such a case, the Provider agrees to inform the SPONSOR of this disqualification by sending an official notification, using a registered letter with a request for acknowledgment of receipt.

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

# 6. Audit

The Provider undertakes to allow the SPONSOR, or any third-party auditor who is not a competitor of the Provider and that the latter would have designated, to review all documents necessary to certify full compliance with the obligations related to conformity with the provisions of Article 28 of the General Data Protection Regulation (GDPR), thereby facilitating the conduct of audits.

By the acceptance of this Service Agreement, the SPONSOR explicitly grants authorization to:

1. The National Agency for the Security of Information Systems (ANSSI) as well as the qualified entity competent to undertake the verification of conformity of the Service and its information system to the SecNumCloud framework.
2. An information systems security audit service provider, fully qualified as PASSI and expressly designated by the Provider, to conduct security audits of the Service.

# 7. Service Description

## 7.1. Shared Responsibility Model

The Service offered by the Provider is characterized by the provision of the following services, which are aligned with the principle of shared responsibility presented in the SecNumCloud framework:

* Provision of computing resources (compute);
* The provision of storage spaces;
* Access to network and internet connectivity services;
* The offering of a backup service dedicated to virtual machines.

The shared responsibility model applied between the Provider and the PRINCIPAL within the framework of the Service is presented in §7.1.

It is understood that the Provider will mobilize its expertise to perform the Services according to best professional practices and in accordance with the requirements of the SecNumCloud framework.

The Service is SecNumCloud qualified (see certification in Appendix).

## 7.2. Detailed Presentation of the Service Scope

| Compute | Computing resource of the SPONSOR Tenant |
| --- | --- |
| Storage | Production data of the SPONSOR Tenant |
| S3 Object Storage | Provision of a sovereign multi-AZ object storage infrastructure compatible with standard S3 APIs. |
| Backup | Subject to subscription to suitable mass-storage |
| Network Infrastructure | Network resource of the SPONSOR Tenant |
| SPONSOR Console | The service enabling the SPONSOR to access and administer their IaaS service via the Shiva interface |
| Support | The support service accompanying the aforementioned services and only those (\*) |

\_(\*) Within the scope of the SNC qualified Service and the responsibilities of the Provider in this regard\_

### 7.2.1. Datacenter Infrastructures

The Service encompasses the provision, for each Availability Zone, of the qualified services listed below:

* Datacenter site located in France for the FR Region, compliant with the latest technological standards, offering a level of resilience equivalent to or greater than the Tier 3 level of the Uptime Institute;
* Provision of technical rooms within datacenters dedicated to hosting the technical equipment essential for the production of the service, including computing, storage, network, cabling, and other necessary components;
* Secured power supply, provided by two distinct electrical circuits, guaranteeing service continuity;
* Provision of air conditioning services, adjusted to comply with the norms and recommendations of equipment manufacturers, to maintain an optimal environment for technical devices;
* Continuous monitoring and detailed metrology, allowing precise tracking and proactive management of the performance and security of the provided service.

The Provider ensures the availability of advanced fire detection and suppression services, designed to effectively identify and neutralize any fire outbreak within the facilities. These systems are essential to guarantee the safety of equipment and data. They include high-precision smoke detectors and extinguishing devices that can quickly act without damaging computer equipment. This service is crucial for preventing fire risks, minimizing potential damage, and ensuring the continuity of operations.

The SPONSOR is informed that all the security procedures and measures in place, including the annual switchover tests on the generators, are essential for ensuring the continuity and integrity of the services provided. These practices are designed to minimize the risk of failure and ensure optimal responsiveness in the event of an Incident. By accepting these conditions, the client acknowledges the importance of these measures and commits to fully cooperate to facilitate their implementation. The SPONSOR is also encouraged to familiarize themselves with the provided security recommendations and integrate them into their own risk management strategy.

### 7.2.2. Software infrastructure for Service management

The Provider supplies the SPONSOR with the administrative console and the API necessary for the use of the Service. It also commits to maintain this administrative console and the API in optimal operational condition and to ensure their security on an ongoing basis. This administrative console and the API are collectively referred to as the “SPONSOR interface.”

The Provider alerts the SPONSOR to the fact that abnormal use of the SPONSOR interface, especially in cases of overloading its command APIs (hammering), can trigger automatic security measures resulting in the blocking of access to the command APIs or to the Service. It should be emphasized that this situation does not constitute a Service unavailability but an action to protect the Service and the Provider’s infrastructure; therefore, the SPONSOR cannot consider it an outage in its calculations.

Furthermore, the Provider specifies to the SPONSOR that perfectly identical requests (duplicates) sent to its APIs are limited to one per second (Throttling). If the SPONSOR submits identical requests at a higher frequency, their rejection cannot be interpreted as a Service unavailability.

### 7.2.3. Computing Infrastructures

The Service includes the provision, in the availability zones subscribed by the SPONSOR, of the necessary equipment for the execution of workloads in the form of virtual machines.

This includes:

* The provision of technical chassis necessary for the proper operation of computing blades;
* The supply of computing blades in the quantities specified by the SPONSOR and distributed according to the availability zones of their choice. It should be noted that these computing blades are exclusively dedicated to the SPONSOR;
* The provision of operating systems of the hypervisor type, as well as the guarantee of maintaining the operational condition and security of the necessary software infrastructure for the management of these operating systems. It is important to highlight that, even though the Provider is responsible for the operational maintenance and overall security of the Service, they do not possess specific knowledge regarding the production environments of the SPONSOR nor the requirements related to its workloads. Consequently, the responsibility to decide on updating the operating systems of the hypervisor computing blades, an action that may require a restart, lies entirely with the SPONSOR. This operation can be carried out via the SPONSOR Interface.

The selection of the computing blade model, chosen from the catalog offered by the Provider, is the responsibility of the SPONSOR.

### 7.2.4. Storage Infrastructure

The service includes providing the SPONSOR with a shared storage infrastructure of the SAN (Storage Area Network) type, offering various levels of performance. This service encompasses:

* The implementation and maintenance in operational and security conditions of the dedicated SAN network;
* The installation and management of storage arrays shared among clients, including maintaining them in operational and security conditions, their supervision, and their metrology;
* The establishment of automated systems for the allocation of LUNs (Logical Unit Numbers) dedicated to the use of the SPONSOR, in accordance with the volumes subscribed to by the SPONSOR.

### 7.2.5. Global Network Infrastructure

The Provider deploys, as part of the Service, a global network facilitating for the SPONSOR the accessibility of its hosted systems. This service includes:

* The provision, operational maintenance, and security of all fiber optic links interconnecting the various Availability Zones;
* The provision, operational maintenance, and security of technical equipment necessary for the proper functioning of the network and the isolation of different clients.

The network interconnection of the SPONSOR Tenant to the Internet or private networks, and the network equipment, carrier links, and other technical components effectuating this interconnection, are not included in the scope of the Service. This network interconnection is implemented in accordance with the provisions set out in the Contract.

### 7.2.6. Backup Infrastructure

The Provider makes available to the CLIENT an integrated, dedicated, and managed backup service designed to protect its virtual machines. The Provider ensures the operational and security maintenance of this backup service. The Provider guarantees that the CLIENT’s backups will be located outside the Availability Zone of the saved workloads, provided that the CLIENT has subscribed to the adequate Work Units.

This backup service is limited to the backup of virtual machines and the topology configurations of the CLIENT’s Tenants IaaS environment within the scope of the Service. The development and implementation of an appropriate backup policy by the CLIENT depend on the subscription to specific Work Units. Therefore, it is the CLIENT’s responsibility to ensure the availability of the necessary technical resources with the Provider to implement their backup policy or to adjust it according to the available means.

The Provider commits to notifying the CLIENT in case of capacity constraints and to provide advisory assistance for resource optimization. The obligations of the Provider will be limited to the implementation of the backup policy needs expressed by the CLIENT, within the framework of the subscribed resources.

### 7.2.7. Implementation of Disaster Recovery or Business Continuity Solutions

The Provider supplies the SPONSOR with all the necessary technical solutions to ensure optimal allocation of its resources across various Availability Zones. It is the responsibility of the SPONSOR to manage this distribution of resources effectively, for which they have the opportunity to utilize the tools made available by the Provider for this purpose.

## 7.3. Limitations of Services in the Qualified IaaS Model

### 7.3.1. Managed Services in RUN

It is important to note that the following are excluded from the Service:

* Hosting of physical components belonging to the SPONSOR;
* Network interconnection of the SPONSOR’s Tenant, to the Internet or private networks, including carrier links;
* Any kind of managed service, or Application Management (TMA);
* Any support for virtual machines at the OS level and above in the IaaS responsibility stack, even if it is mere supervision.

However, it is absolutely not excluded that the SPONSOR may use such services from the Provider’s MSP offerings to carry out managed services on its Tenants. These services will then not be governed by this Service Agreement and its bi-partite commitments/clauses.

### 7.3.2. Disaster Recovery Configuration

By default, the Provider sets up the IaaS resources for the SPONSOR by reserving resources and configuring deployments to use Availability Zones. It is the responsibility of the SPONSOR to select the Availability Zones through the SPONSOR interface.

### 7.3.3. Backup Configuration

The backup service is limited to the backup of virtual machines and topology configurations representing the IaaS environment of the SPONSOR’S Tenants as part of the Service.

The provision of the backup service and the completion of the SPONSOR’S backup policy is subject to subscription for storage space on the mass storage needed to ensure the service. It is therefore the responsibility of the SPONSOR to subscribe to the necessary technical means from the Provider to ensure the backup policy on its IT perimeter, or to adjust the backup policy to the means implemented. The Provider commits to inform the SPONSOR in case of technical capacity limits.

The Provider will implement the technical and human means necessary for the backup of the hosted system within the limit of resources subscribed by the SPONSOR.

Furthermore, in the case of perimeters not covered by the Provider, it is up to the SPONSOR to define its own backup strategy and to configure the backups of the VMs by itself or to make a Service Request to the Provider so that the setup of backups for physical servers can be implemented if the SPONSOR has a managed service contract allowing the Provider to act via the SPONSOR interface which is the administration console provided as part of this Service Agreement and has functionalities to configure backups.

Moreover, this service will only commit to reflect through the configuration via the SPONSOR interface, the configuration clearly specified by the SPONSOR.

For the flexibility of the Provider’s offering, the SPONSOR has the option to associate a no-backup policy with some of its VMs. In this case, it is up to the SPONSOR to assume this choice. The Provider will not backup the VMs associated with the “no backup” policy. The Provider alerts the SPONSOR that choosing the “no backup” policy or choosing to backup manually exposes the SPONSOR to a permanent data loss in the event of an Incident on the low layers or on layers depending on its responsibility in the IaaS model. In such a case, it will be impossible to hold the Provider responsible for restoring the data as there will be nothing to restore. The Provider recommends always backing up the VMs.

For any matter concerning the OS installed on a virtual machine and any software or program executed “above the OS,” it is the responsibility of the SPONSOR to carry out administration and supervision operations within the European Union if they wish to ensure that all vertical layers of the IT system are operated and managed from the European Union. Administration operations outside the responsibility perimeter of the Provider as part of this Service Agreement are indicated in the “Shared Responsibilities Model” section of this Service Agreement.

## 7.4. Implementation of the service

### 7.4.1. Technical Prerequisites

For the implementation of the Service, the SPONSOR acknowledges that it must:

* Operate with VMware type virtualization in versions supported by the publisher and provided by the Service Provider as part of the Service;
* Use, through the Service Provider, the backup tool;
* Declare fixed IPs from which the Service Provider will authorize access to the SPONSOR interface (Whitelist filtering). Modifications to this list of IPs must be made via Service Requests (list not manageable from the Service administration interface).

## 7.5. Service Localization in France

It is specified that none of the operations and none of the physical components involved in the provision of the Service, which this Service Agreement concerns, are located outside of the European Union.

This includes, in particular, support, operational supervision, and security oversight (SOC) of the technical infrastructure delivering the Service. Indeed, all storage, all administrative tasks, supervision, and processing are carried out in France.

### 7.5.1. Location of Datacenters Hosting the Service

In the absence of the operations of the collaborators and the service provider’s agencies, all production operations (which include data storage and processing) and technical components delivering the Service are located in Datacenters based in France.

### 7.5.2. Location of Cloud Temple Agencies Operating the Service

Cloud Temple employees working within the scope of the Service operate from Cloud Temple’s offices, all of which are located exclusively in France. These offices are in France, specifically in Tours, Lyon, Caen, and Paris La Défense.

The CLIENT is informed of the possibility for Cloud Temple employees to work remotely. However, the Provider guarantees the same level of security for remote access, particularly concerning VPN access. These remote accesses are implemented in accordance with the requirements of the SecNumCloud standard.

## 7.6. Support

### 7.6.1. Nature of Support Accompanying the Service

The Provider offers a technical support service aimed at assisting the SPONSOR in managing, troubleshooting, and optimizing their deployed resources. This service covers an extensive range of activities, from assistance with the initial configuration of services to advanced technical support for resolving specific issues.

Here is a description of the characteristics and functionalities of the support service:

* Assistance with the initial implementation of the Service usage;
* Assistance with incident resolution;
* Assistance with problem solving;
* Monitoring and advice on the technical base optimization.

Under the support service, the Provider does not replace the SPONSOR in using the Service. The SPONSOR remains fully responsible for the configuration, operation of their VMs and Tenants, and management of all elements (including data and applications) they have stored or installed on the Provider’s infrastructures. Technical support service is provided in accordance with the General Conditions of Sale and Use, the Provider being bound by a duty of means.

The SPONSOR agrees to use the technical support service reasonably, refraining from requesting services not subscribed to from the Provider and from involving the Provider’s teams with its own clients or third parties not included in the Contract. The Provider reserves the right to reject any service request that does not respect these criteria.

The level of commitment of the support is conditioned to the subscription of the associated support task units.

### 7.6.2. Requesting technical support service

Technical support is accessible through a ticketing system via the SPONSOR console and is available during normal business hours excluding public holidays (8 a.m. - 6 p.m.; Monday – Friday; French calendar and schedule). For emergencies occurring outside business hours, particularly incidents significantly affecting production, an on-call service can be reached via a number communicated to the SPONSOR when initializing the Service.

For each request or Incident, it is imperative to generate a ticket with the Provider’s support. The initialization of this ticket, containing all necessary information, is essential and marks the beginning of the assessment of the Provider’s commitments.

As soon as the Provider receives a request or an Incident notification, whether through the management console or following a telephone call, a ticket is automatically created. When reporting an Incident, it is essential that the SPONSOR provide the provider with as many details as possible about the problem encountered. This approach is crucial to allow an adequate assessment of the situation, prioritization, and an effective diagnosis.

The Client then receives an email confirmation, indicating the creation of the ticket and its unique number. The SPONSOR can consult the status and history of their requests and Incident declarations directly from the management console.

### 7.6.3. Incident Management Process

When reporting an Incident, the technical support team of the Service Provider initiates an investigation to identify the cause of the problem and establish a diagnosis. The Client must actively collaborate with the Service Provider by providing all the necessary information and performing the required tests. The Service Provider may access the Client’s Service to diagnose the Incident.

If the Service Provider’s Services are deemed operational and the Incident is not attributable to them, the Client will be informed. At the request of the Client, the Service Provider may offer Professional Services to identify the source of the problem, billable upon prior agreement in 30-minute increments.

In the event that the Incident is the responsibility of the Service Provider or one of its subcontractors, the provider completes the diagnosis and sets about restoring the Service at no additional cost. The diagnosis relies on the exchanges between the Parties and the data of the Service Provider, these elements being considered conclusive by agreement of the Parties.

### 7.6.4. Prioritization Process of Treatments

Determining the priority level of a file is based on a matrix analysis that assesses the impact of the incident and its degree of criticality:

* The Impact levels are defined as follows:

| Level of Impact | Description |
| --- | --- |
| Impact I1 | The service or services provided by the Contractor are interrupted |
| Impact I2 | The service or services provided by the Contractor are degraded |
| Impact I3 | The service or services provided by the Contractor are currently stable but show signs of potential long-term decline |

* The levels of Criticality are defined as follows:

| Level of Criticality | Description |
| --- | --- |
| Criticality C1 | The service or services provided by the Contractor deteriorate at an alarming rate |
| Criticality C2 | The service or services provided by the Contractor progressively deteriorate over time |
| Criticality C3 | The service or services provided by the Contractor present one or several minor issues without significant consequences |

* Based on a thorough analysis of the situation, taking into account the elements determining Impact and Criticality, a priority is assigned to the ticket in accordance with the following decision matrix:

| Level of Impact  Level of Criticality | Impact I1 | Impact I2 | Impact I3 |
| --- | --- | --- | --- |
| Criticality C1 | Priority **P1** | Priority **P2** | Priority **P3** |
| Criticality C2 | Priority **P2** | Priority **P3** | Priority **P4** |
| Criticality C3 | Priority **P3** | Priority **P4** | Priority **P5** |

The service level commitments corresponding to each priority level are detailed in the following chapter.

### 7.6.5. Language and localization of the support service

Support is provided by the Service Provider to the SPONSOR at a minimum in the French language. Support may also be provided in English.

The operations of the Service Provider’s support service for the qualified SecNumCloud infrastructure service offering are located within the European Union.

# 8. Commitments and Service Levels

The Service Provider commits to guaranteeing continuous monitoring of the performance and security integrity of its technical infrastructure that delivers the Service, ensuring their optimal functioning.

The unavailability of a service, which is the subject of a performance indicator, is acknowledged as soon as it is identified by the Service Provider’s monitoring system, or following a notification by a user of the SPONSOR. The start of the unavailability is fixed at the earliest moment between these two events, in order to guarantee an accurate and fair accounting of the downtime.

The end of the unavailability is officially marked by the full restoration of the service, confirmed either by the Service Provider’s monitoring tools or by user feedback, thus ensuring an effective resumption of operations and a faithful measurement of the duration of the interruption.

## 8.1. Service Infrastructure Availability Commitments

The Provider undertakes to maintain a level of availability and performance in accordance with the standards defined for each specified period. The service level commitments (Service Level Agreements, SLAs) apply provided that the SPONSOR implements its systems across at least two of the Availability Zones present in the concerned Region.

In the absence of meeting these conditions by the SPONSOR, they will be unable to claim the application of the concerned SLAs, which are specifically identified with an asterisk (\*). Accessibility to SLAs is through the SPONSOR interface. Measures are understood to be calculated monthly:

* **SLA 1 (\*): IC-INFRA\_SNC-01** – Compute power availability: guaranteed availability rate of 99.99%, calculated on a 24/7 basis.
* **SLA 2 (\*): IC-INFRA\_SNC-02** – Storage availability: guaranteed availability rate of 99.99%, calculated on a 24/7 basis.
* **SLA 3: IC-INFRA\_SNC-03** – Backup reliability: guaranteed availability rate of 99.99%, calculated on a 24/7 basis.
* **SLA 4 (\*): IC-INFRA\_SNC-04** – Network infrastructure availability: guaranteed availability rate of 99.99%, calculated on a 24/7 basis.
* **SLA 5: IC-INFRA\_SNC-05** – Internet access: guaranteed availability rate of 99.99%, calculated on a 24/7 basis.

***Remarks***:

* *In response to a distributed denial of service (DDoS) attack, the Provider reserves the right to adjust its internet routing configuration to limit the impact of this attack and safeguard its infrastructure. In particular, if an IP address belonging to the SPONSOR is targeted, the Provider may resort to the blackholing technique via the BGP community to block all traffic to the targeted IP address upstream at its suppliers, with the aim of protecting the resources of the SPONSOR as well as those of other SPONSORs and of the Provider’s infrastructure. The Provider strongly encourages the SPONSOR to adopt similar measures, such as the use of web application firewall software available on the market, and to carefully configure their security groups via the command API.*
* *The Provider insists on the need for the SPONSOR to minimize the opening of flows, in particular by avoiding making the administration ports* ***SSH*** *(TCP port 22) and* ***RDP*** *(TCP port 3389) accessible from the whole internet (subnet 0.0.0.0/0), as well as internal protocols such as* ***SMB*** *(TCP/UDP port 445) or* ***NFS*** *(TCP/UDP port 2049).*

## 8.2. Availability commitment of the SPONSOR interface

* SLA 6: IC-INFRA\_SNC-06 – Access to the Service Administration Console: a guaranteed availability of 97%, ensured continuously, 24 hours a day and 7 days a week.
* SLA 7: IC-INFRA\_SNC-07 – Access to the Service Control APIs: a 99.9% availability, calculated on a 24/7 basis.

## 8.3. Availability Commitment of Support

* **SLA 8 : IC-INFRA\_SNC-08** – Here are the technical support performance commitments from the Provider for incidents, excluding scheduled maintenance:

| Priority | Guarantee of Intervention Time (GIT) | Performance Objective |
| --- | --- | --- |
| Priority **P1** | 30min | 95% |
| Priority **P2** | 2h | 90% |
| Priority **P3** | 4h | 90% |
| Priority **P4** | 24h | 85% |
| Priority **P5** | 48h | 85% |

* **SLA 9 : IC-INFRA\_SNC-09** – Here are the technical support performance commitments from the Provider for service requests:

| Service Request | Guarantee of Intervention Time (GIT) | Performance Objective |
| --- | --- | --- |
| Service request | 4h | 90% |

*Note*:

* *The time frame for the Guarantee of Intervention Time (GIT) is calculated from the difference between the moment the SPONSOR opens the ticket and the first intervention by the Provider’s support.*
* *Incident investigation concerning the SPONSORs will not include remote intervention on the SPONSORs’ hosted servers. This assistance will be limited to the explanation of available metrics related to the SPONSOR’s environment, with the aim of facilitating understanding of the incidents or performance problems encountered. Based on the results of this analysis, recommendations may be suggested.*

## 8.4. Commitment to S3 object storage availability

* **SLA 10 : IC-INFRA\_SNC-10** – Here are the availability commitments for S3 object storage:

| Indicator | Commitment | Availability Objective |
| --- | --- | --- |
| IC-INFRA-SNC-10.1 | Storage durability of an object within a region | 99.9999999% / year |
| IC-INFRA-SNC-10.2 | Availability of the S3 Object Storage API | 99.99% |
| IC-INFRA-SNC-10.3 | Maximum latency for accessing an object in a region | 150 ms |

Remarks:

* The Object Storage Service is specifically designed for object storage and should only be used for this purpose, **categorically excluding its use in block mode**. Any resort to block mode through indirect methods, including for example the use of *“FUSE” in a Linux environment*, constitutes a breach of the terms of use set out. No incident, malfunction, or damage resulting from this non-compliant usage will be covered by the Service Level Agreements (SLAs) defined in this service agreement.
* The durability guarantee is conditional upon the use of services in compliance with current best practices and standards, and explicitly excludes any data modification, whether intentional or accidental, resulting from actions taken by the SPONSOR.

## 8.5. Clarification regarding the backup commitment

The backup strategy deployed for the SPONSOR is conditioned by the subscription to the appropriate work units.

The Service Provider commits to providing a backup solution that will allow the SPONSOR to apply the desired backup policies.

It is specified that the scope of the Service Provider stops at providing a backup service, and it is the responsibility of the SPONSOR to oversee, via the SPONSOR interface, the proper execution of the associated policies.

It is also specified that the management of storage capacity for the storage space dedicated to backups remains the responsibility of the SPONSOR. The Service Provider makes the usage rate available through the console.

*Example: Non-backup of a virtual machine:*

*The SPONSOR is responsible for verifying/supervising the proper execution of the backup policies. In the event that the SPONSOR notices that a virtual machine is not backed up, it is their responsibility to check the cause. The SPONSOR may request the Support of the Service Provider according to the level of support subscribed to be assisted.*

**SLA 8: IC-INFRA\_SNC-08** and **SLA 9**, will be exclusively applicable in the event of an Incident with the backup service.

# 9. Organization of the Contractual Relationship

## 9.1. Provider’s Responsibilities

The Service Provider commits to:

* Adequately inform its SPONSOR (for example, in case of limited capacity of technical resources delivering the Service).
* Formally inform the SPONSOR, within a period of one month, of any legal, organizational, or technical change that may impact the compliance of the Service with the requirements of protection against non-European laws (19.6 of the SNC v3.2 standard).
* Provide to the SPONSOR service interfaces and interfaces that are at least in the French language.
* Study and take into account the specific sectoral requirements related to the types of information entrusted by the SPONSOR in the implementation of the service, within the limits of the Service Provider’s responsibilities.
* Not disclose any information related to the service to third parties, except with formal and written authorization from the SPONSOR.
* Provide all necessary information for the performance of compliance audits in accordance with the provisions of Article 28 of the GDPR.
* Report to the SPONSOR, through this Service Agreement, any security incident impacting the Service or its use by the SPONSOR (including the SPONSOR’s data).
* Allow a qualified Information Systems Security Audit Provider (PASSI), mandated by the Service Provider, to audit the service as well as its information system, in accordance with the Service Provider’s SecNumCloud control plan. Furthermore, the Service Provider commits to providing all necessary information to successfully carry out compliance audits with the provisions of Article 28 of the GDPR, conducted by the sponsor or a third party mandated.
* Provide, as a subcontractor and in accordance with Article 28 of the General Data Protection Regulation (GDPR), assistance and advice to the SPONSOR by alerting them as soon as an instruction issued by the latter is likely to constitute a violation of data protection rules.
* Notify in writing, when a project affects or is likely to affect the security level of the Service, the SPONSOR of potential impacts, mitigation measures implemented, as well as the residual risks concerning them.
* Document and implement all necessary procedures to meet the legal, regulatory, and contractual requirements applicable to the service, as well as the specific security needs of the SPONSOR, defined by them and provided for in the Contract. At the request of the SPONSOR, the Documentation module of the SPONSOR interface will allow for secure sharing of these documents.
* Provide, upon SPONSOR’s request, risk assessment elements related to the submission of the SPONSOR’s data to the law of a non-European Union state.

Upon formal and written request from the SPONSOR, the Service Provider commits to:

1. Making available to the SPONSOR the internal regulations and the code of ethics of the Service Provider;
2. Providing the SPONSOR access to the penalties incurred in case of infringement of the security policy;
3. Providing the SPONSOR with all events concerning them within the logging elements of the Service;
4. At the end of the Contract, the Service Provider commits to deleting the data and technical data related to the SPONSOR, in accordance with the “data erasure procedure at the end of the Contract” described in this Service Agreement.
5. Ensure secure erasure of all the SPONSOR’S data by completely rewriting any medium that hosted their data within the framework of the Service.
6. Provide the complete list of authorized third parties to access the data infrastructures.

The Service Provider will maintain an updated list and make it available to the SPONSOR of all third parties authorized to access the data infrastructures, informing them of any change related to the subcontractors. The Service Provider and all its subsidiaries commit to respect the fundamental values of the European Union, namely human dignity, freedom, democracy, equality, the rule of law, as well as the respect for Human Rights. The service provided by the Service Provider complies with current legislation in terms of fundamental rights and the values of the European Union regarding respect for human dignity, freedom, equality, democracy, and the rule of law.

## 9.2. Limitation of the Service Provider’s Liabilities

Due to the definitions and conditions mentioned in the present Service Agreement, the responsibilities of the Provider are limited as follows:

1. The shared responsibility model, described in the “Shared Responsibilities Model” section of this Service Agreement, effectively limits the Provider’s involvement in the operating layers that go “above” the provision of computing resources, network, storage, and backup. This excludes, in particular but without limitation:
   * The management of what is installed on virtual machines (OS, middlewares, applications, etc.);
   * Updating the OS and other software installed by the SPONSOR on its machines in its Tenants;
   * The security of the programs, software, and applications installed on virtual machines;
   * Updating the virtual machines;
   * Application-level data backup.
2. The Provider cannot commit to backing up the SPONSOR’s Tenants unless the SPONSOR has previously subscribed to the appropriate work units.
3. The Provider cannot claim ownership of the data transmitted and generated by the SPONSOR. Indeed, they are the property of the SPONSOR.
4. The Provider emphasizes that it cannot in any case exploit the data transmitted and generated by the SPONSOR without prior validation from the latter.
5. The Provider disclaims all responsibility for components that are physically hosted and managed by the Provider but are the direct property of the SPONSOR or a third party with whom the SPONSOR has contracted. The hosting of clients’ physical components is not part of the Service and is therefore outside the scope of this Service Agreement. It is the responsibility of the SPONSOR to assess the level of adherence or dependency that these components introduce with respect to the SecNumCloud qualified IaaS Service.

## 9.3. Access Limitation

As part of the Service, the Provider is formally prohibited from accessing Tenants belonging to the CONTRACTING PARTY without prior authorization. It is the responsibility of the CONTRACTING PARTY to provide the necessary access to the Provider’s personnel, according to the specific needs of the hosting and, if applicable, professional support services, if this option has been selected by the CONTRACTING PARTY.

The CONTRACTING PARTY acknowledges that these accesses are granted exclusively for the needs related to the agreed service provision, ensuring secure management that is compliant with the terms of the agreement.

Remote access by third parties involved in the Provider’s service provision is strictly prohibited. In the event that a specific technical requirement would necessitate such access, it can only be established after clearly notifying the CONTRACTING PARTY, providing a detailed justification, and obtaining their written agreement.

This measure ensures the control and security of the CONTRACTING PARTY’s data, by making certain that any exceptions to the rule are duly authorized and documented.

## 9.4. Responsibilities of Third Parties Participating in the Provision of the Secure Temple Service

The Provider is proficient in the list of third-party partners involved in the provision of the Service. These third parties are publishers, suppliers (of the Provider), and other vendors participating in the provision of the Service. The Provider implements the following measures with these third parties:

* The Provider requires third parties involved in the implementation of the service, in their contribution to the Service, a level of security at least equivalent to that which it commits to maintain in its own security policy applicable to the Secure Temple service;
* The Provider contracts with each of the third parties involved in the implementation of the service, audit clauses allowing a qualification body to verify that these third parties comply with legal requirements and SNC requirements, enabling the Provider to fulfill its commitments in the present Service Agreement.
* The Provider implements a procedure to regularly control the measures put in place by third parties involved in the implementation of the service to meet the requirements for the Provider to honor its commitments in the present Service Agreement.
* The Provider implements a procedure for monitoring changes made by third parties involved in the implementation of the service that may affect the security level of the service’s information system.

## 9.5. Responsibilities and obligations of the SPONSOR

For reference, the Service Provider provides the CLIENT with a virtual machine execution platform; the CLIENT is responsible for configuring these machines. Each virtual machine cannot operate without an associated backup policy. The Service Provider defines automatic backup policies via its interfaces. However, it is the CLIENT’s responsibility to activate these backup policies and thus enable the virtual machines.

The CLIENT authorizes ANSSI and the SNC qualification organization to audit the Service and the technical infrastructure delivering the Service.

## 9.6. Rights of the CLIENT

At any point during the contractual relationship, the SPONSOR may file a complaint related to the qualified service with the ANSSI.

At any time, the SPONSOR may request the Service Provider to make its internal regulations and ethical charter accessible to them.

## 9.7. Data Deletion at the End of the Contract

Upon the conclusion of the contract, whether it expires or is terminated for any reason, the Service Provider undertakes to perform a secure deletion of all the data of the SPONSOR, including technical data. The Service Provider will ensure to provide the SPONSOR with a formal notice, respecting a period of twenty-one (21) calendar days. The SPONSOR’s data will then be deleted within a maximum period of thirty (30) days following this notification.

To attest to this deletion, the Service Provider will issue a certificate to the SPONSOR confirming the erasure of the data.

# 10. Life Cycle of the Current Service Agreement

## 10.1. Entry into Effect of the Service Agreement

The present Service Agreement comes into effect on the date of its signature by the SPONSOR.

The collection, handling, storage, and processing of data carried out within the framework of pre-sales, implementation, and termination of the Service, are conducted in compliance with current legislation.

## 10.2. Amendments to the Service Agreement

Amendments or additions to this Service Agreement exclusively result from requests made by the governance bodies designated for this purpose. These proposed changes will be reviewed by the Parties, who are authorized to determine aspects that require written formalization.

It is agreed that any evolution of the Service Agreement, after approval, that alters the initial financial conditions, will require the establishment and signing of an amendment to the current Contract.

Factors that may induce a review of this Service Agreement include, but are not limited to:

* Changes in the technical infrastructure delivering the IaaS Service;
* Adjustments made to the services deployed by the Provider to deliver the Service;
* Variations of commitments made and applicable penalties;
* Organizational reconfigurations within the SPONSOR or the Provider;
* Expansion or reduction of the scope of the Service.

The management of versions and revisions of the Service Agreement is recorded in the preamble of the document to facilitate tracking.

### 10.2.1. Evolutions Triggered by the SPONSOR

Service Agreement Amendments may stem from, specifically:

* An evolution of the infrastructure managed by the Service Provider;
* A change in the services implemented by the Service Provider;
* A revision of the service level commitments by the Service Provider.

### 10.2.2. Amendments Initiated by the Service Provider

Any modification to the Service Agreement is subject to the SPONSOR’s acceptance. It is understood that any validated modification or addition altering the financial elements of the Contract may involve the signing of an amendment to it.

## 10.3. Reversibility

Additionally, Cloud Temple commits to allowing a revision of this Service Agreement (including its termination) without penalty for the SPONSOR in the event of loss of the SecNumCloud qualification.

The Services do not include an obligation of reversibility (that is, assistance to the Client to migrate their system to another service provider) except for making available to the SPONSOR by the service provider, an SPONSOR interface that allows the SPONSOR to back up and retrieve their data, including specifically the configuration data of their information system through one of the following technical options at the SPONSOR’s choice: the provision of files in one or more documented formats that can be used outside of the service provided by the service provider or through the establishment of technical interfaces that allow access to data according to a documented and usable scheme (API).

The SPONSOR, sole master of their system, must do everything possible to facilitate this operation as needed (which implies, in particular, that they must establish rigorous documentation to this effect) and the development of reversibility plans. In the event that the SPONSOR would need an additional service, the service provider may offer consulting services in this regard within the framework of a specific contract to be negotiated.

# 11. Availability, Continuity, and Service Restoration

## 11.1. Incident and Interruption Management

### 11.1.1. Incidents

#### 11.1.1.1. Types of Incidents Addressed Under this Service Level Agreement

* Disasters
* Breakdowns and Failures
* Security Incidents:
* Affecting service availability
* Affecting service confidentiality
* Affecting service integrity

#### 11.1.1.2. Incident Management

* Deadlines
* Post-mortem Actions
* Archive the documents detailing security incidents.
* Personal Data Breach Notification (online): <https://notifications.cnil.fr/notifications/index>

#### 11.1.1.3. Security Incident Notification Level

The SPONSOR has the responsibility to choose the severity levels of Security Incidents for which they wish to be informed, for example through their formalization in an SLA applicable to the Service.

By default, the SPONSOR is informed:

* Of security incidents with impact (impacts I1 and I2 according to the impact scale defined in the process of prioritizing treatments of the present Service Agreement);
* Of personal data breaches for which the SPONSOR is responsible for the processing;
* Of personal data breaches for which the Provider is responsible for the processing and involving personal data of the SPONSOR.

## 11.2 Service Maintenance

### 11.2.1. Nature of Maintenance

The maintenance provided consists of the implementation of:

* The plan to maintain operational conditions of the Service to ensure good availability indicators as committed by the Supplier above;
* The Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) if subscribed to by the SPONSOR, triggered according to any incidents that might occur.

### 11.2.2 Remote Access by Cloud Temple to the SPONSOR’s Scope

In the context of this Service Agreement, the Service Provider is prohibited from accessing the Tenants and the COMMANDITAIRE’s interface space.

It will be the responsibility of the COMMANDITAIRE to provide the necessary access to the Service Provider’s personnel. The COMMANDITAIRE acknowledges that the access will be used in the context of hosting and ultimately managed services (if subscribed to by the COMMANDITAIRE).

### 11.2.3. Remote Third-Party Access Participating in the Service Provision within the COMMANDITAIRE’s Scope

No remote access by third parties involved in the provision of the Service is permitted.

Should a technical need make this scenario necessary, such access would only be carried out after notification to the SPONSOR with justification and obtaining their written consent.

# 12. Procedure for Data Deletion at the End of the Contract

Upon termination of the Contract, whether the Contract has expired or for any other reason, the Service Provider shall ensure the secure erasure of all data processed as part of the Service, including the technical Data of the CLIENT. The Service Provider will give formal notice respecting a period of twenty-one (21) calendar days. The CLIENT’s data will be deleted within a maximum period of thirty (30) days after the notification. The Service Provider provides a data deletion certificate to the CLIENT.

# 13. Applicable Law

## 13.1. In General

The applicable law and to which this Service Agreement is subject is French law.

## 13.2. Compliance with Applicable Laws and Regulations

The Service Provider commits to the following points:

* Identification of the applicable legal and regulatory constraints within the framework of the Service;
* Compliance with the legal and regulatory constraints applicable to the data entrusted to the Service Provider;
* Compliance with the Data Protection Act and the GDPR;
* Implementation of means for the protection of personal data;
* Implementation of a legal and regulatory monitoring process;
* To have and maintain appropriate relationships or monitoring with the sectoral authorities related to the nature of the data processed within the framework of the Service. This includes in particular the ANSSI, the CERT-FR, and the CNIL.

## 13.3. GDPR

Acting as a subcontractor within the meaning of Article 28 of the General Data Protection Regulation (GDPR), the Service Provider undertakes to:

* Ensure transparency and traceability;
* Appoint a DPO in charge of defining and implementing measures to protect personal data;
* Provide assistance and advice to the CLIENT by alerting them if any instruction constitutes a violation of personal data protection rules if the Service Provider is able to identify it;
* A guarantee of security on the processed data (due to the SecNumCloud qualification).

## 13.4. Protection Concerning Non-European Law

If the Provider resorts to the services of a third-party company - including a subcontractor - with its statutory headquarters, central administration or main establishment in a non-member state of the European Union or owned by or under the control of a third-party company located outside the European Union, within the framework of the Service, the Provider undertakes that said third-party company shall not have any access to the data processed by the ‘Secure Temple’ service.

For reference, the targeted data are those entrusted to the Provider by the PRINCIPAL as well as all Technical Data including information about the PRINCIPALS.

For the purposes of this article, the notion of control is as defined in II of Article L233-3 of the commercial code.

# 14. SIGNATURES

Done at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For Cloud Temple, the PROVIDER

For \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, the SPONSOR