**SECNUMCLOUD SERVICE AGREEMENT**

**BETWEEN THE UNDERSIGNED,**

OUTSCALE, a simplified joint stock company with a capital of €1,849 930, registered at the Nanterre trade and companies registry under the number n° 527 594 493, having its registered office at sis 1, rue Royale, 319 Bureaux de la Colline, 92210 Saint-Cloud, represented by David CHASSAN duly empowered for the purposes hereof in his capacity as Chief Strategy Officer,

hereafter referred to as“**the Service Provider**”or“**3DS OUTSCALE”,**

**ON THE ONE HAND,**

**and**

*Fill in the information on the identity of the contracting party (corporate name, domiciliation, representative, registration n° if applicable.*

hereafter referred to as“**the CLIENT**”,

**ON THE OTHER HAND.**

3DS OUTSCALE and the CLIENT being referred to individually as the “Party” and collectively as the “Parties”.

Preamble

3DS OUTSCALE is a French cloud computing services provider working with infrastructures situated in France. 3DS OUTSCALE offers a series of IaaS, PaaS and SaaS services that are secure, innovative and flexible.

L’Agence Nationale de la Sécurité et des Systèmes d’Information (“ANSSI”), France’s national cybersecurity agency, has established a “SecNumCloud” label with a list of requirements applicable to cloud computing services providers who apply for qualification.

This label provides clients who choose SecNumCloud qualified service providers with guarantees as to the aptitude of the service provider and its staff, in terms of the quality of service and the trust that the client can place in the service provider.

The Parties have entered into an Agreement comprising 3DS OUTSCALE’s General Terms and Conditions of Sale and Use, completed by this Service Agreement for the supply of Services within the “Public Sector” Region.

As an exception to the General Terms and Conditions of Sale and Use, in the event of contradiction between the latter and this Service Agreement, the Service Agreement shall prevail.

**3DS OUTSCALE obtained SecNumCloud qualification from l’Agence Nationale de la Sécurité et des Systèmes d’Information (“ANSSI”) under decree n°2015-350 of March 27, 2015, for its *IaaS – CLOUD ON DEMAND* cloud computing services, a copy of said certification being attached to this Service Agreement hereafter (Appendix B). 3DS OUTSCALE is able to provide said IaaS services in accordance with the SecNumCloud label requirements.**

1. Definitions

The terms and expressions identified below beginning with a capital letter shall have the meaning attributed to them in this article, in the specific agreement or in 3DS OUTSCALE’s General Terms and Conditions of Sale and Use to which this Agreement is related.

For the purposes of interpreting this Services Agreement, the Parties have agreed on the following definitions which complete those of the specific agreement or of 3DS OUTSCALE’s General Terms and Conditions of Sale and Use:

**Acts of administration:** All acts involving the installation, removal, modification and consultation of the setup of a system that is part of the Service’s Information System and which may alter its functioning or security.

**Administrator:** A user with special rights allowing them to carry out the tasks assigned to them. There are several categories of Administrator:

* **Security administrator:** Administrator in charge of the security setup, in particular the management of the Administrators’ access rights.
* **Infrastructure administrator:** Administrator in charge of managing the Service’s Technical Infrastructure, keeping it in good working order and ensuring it is secure. The Infrastructure administrator always operates under the responsibility of the Service Provider.
* **System administrator:** Administrator of the logical resources supported by the Service’s Technical Infrastructure. Depending on the type of architecture used for the Service, system administration may concern abstract resources (virtual machines, virtual networks, etc.), operating systems, middleware, business software solutions, etc.
* **Functional system administrator:** Administrator in charge of functional administration at application level.

**Audit:** Systematic, independent and documented process with the aim of obtaining proof and assessing it objectively to determine the extent to which the label’s specific requirements are met.

**Asset:** Any element with a value for the Service.

**3DS OUTSCALE’s General Terms and Conditions of Sale and Use:** adopted between 3DS OUTSCALE and its CLIENT to regulate the Services linked to a CLIENT Account and which can be consulted at the following address <https://fr.outscale.com/cgucgv/>.

**Agreement:** Contractual arrangement comprising a specific agreement or 3DS OUTSCALE’s General Terms and Conditions of Sale and Use, completed by this Service Agreement for the supply of Services in the “Public Sector” Region.

**Service Agreement:** This document in application of the specific agreement or 3DS OUTSCALE’s General Terms and Conditions of Sale and Use and in accordance with the SecNumCloud label requirements.

**Cloud computing:** A method that provides easy access, generally on demand, via a network, to a set of shared and configurable computing resources.

**Availability/uptime:** Ability to make a Service available, with the expected level of service specified in the provisions of the SLA.

**Durability:** Probability of non-deletion of data inadvertently (the deletion could be caused by a physical phenomenon such as “bit flips”, the dysfunction of a specific technology, the aging of the storage media, etc.), for example a sustainability of 99.9999999% per year shall mean that 0.0000001% of the data, at the most, could be altered during the year.

**State-of-the-art:** Set of good practices, technologies and reference documents relating to information systems security accessible to the public, and information that can clearly be derived therefrom. These documents may be put online by the information systems security community, published by reference organizations or be part of the regulatory documentation.

**Information Security Incident:** One or more events linked to information security that are adverse or unexpected, with a strong probability of compromising operations linked to the organization’s business activities or threatening information security.

**Threat:** Potential cause of an adverse incident that could harm a system or organization.

**Security Measure:** Measure that modifies the likelihood or severity of a risk. This includes the policy, procedures, guidelines and practices or organizational structures, and can be administrative, technical, managerial or legal.

**Penalties**: penalties related to the SLA, such as provided in Appendix A of 3DS OUTSCALE’s General Terms and Conditions of Sale – “Penalties related to SLA”.

**Policy:** The expression of an organization’s intentions and orientations, as defined by its management.

**Information Systems Security Auditor:** Entity conducting audits on information systems security. The entity is considered as an approved auditor if a certification body has concluded that its information systems security auditing services meet the requisite standards.

**Quality of Service/SLA:** 3DS OUTSCALE’s quality of service commitments, for example levels of uptime relating to the Service(s).

**SecNumCloud label**: label corresponding to the list of requirements to be met by cloud computing (SecNumCloud) Service Providers, version 3.1 of June 11, 2018, published by ANSSI which applies to this Agreement.

**3DS OUTSCALE/CLIENT Manager:** The representative of 3DS OUTSCALE and of the CLIENT in the framework of the Agreement and this Service Agreement in application thereof. The Managers must have the technical skills required and the legal capacity to bind their company: they are the recipients of the Notices issued in the framework of the Service Agreement. The Managers are defined in the “Contact Persons” article of this Service Agreement.

**Virtualized Resources:** Abstraction of a system’s hardware resources (CPU, RAM, etc.) which are made available by the technical infrastructure.

**Reversibility:** The procedures to be carried out by 3DS OUTSCALE, and by the CLIENT, in the event of the termination of the Agreement, so that the CLIENT can transfer its Data, programs, applications, etc. to another service provider in accordance with the “Reversibility” article of this Services Agreement.

**Risk:** The effect of uncertainty on certain objectives. It is expressed in terms of the combination of the consequences of an event and of its probability.

**Information Systems Security:** All the technical and non-technical means of protection, allowing an Information System to withstand events likely to compromise the availability, integrity and confidentiality of data processed or transmitted and the related services that these systems offer or make accessible.

**3DS OUTSCALE Service(s) or Service(s):** The IaaS services ordered by the CLIENT in the framework of the Agreement and subject to this Service Agreement in application thereof.

**Supervision:** Monitoring of an Information System or Service. This concerns the collection of data (measurement, alarms, etc.) but does not include taking action in respect of the element monitored (which is an Administration task).

**Technical Support (or Support):** All the diagnostic activities whose aim is to resolve the problems encountered by the CLIENT. The tasks carried out by the teams in charge of support fall within the Supervision category. If the resolution of the problem requires action on the part of the Service Provider, this action is the responsibility of Administration and must be carried in the appropriate conditions.

**Information System:** Organized set of resources (hardware, software, personnel, data and procedures) used to process and circulate information.

**Third Parties:** All those participating in the implementation of the Service (host, developer, integrator, archiver, on-site or remote subcontractor, air conditioning suppliers, etc.) listed in article 5 of this Service Agreement.

**User:** Any person with a Cloud Access Account in the scope of the Service. This generic term includes End Users and Administrators.

**End User:** Person who ultimately makes use of the Service implemented. This may be the CLIENT’s personnel in the case of an internal service, or its own clients in the case of an external service.

**Vulnerability:** Weakness of an asset or a measure that can be exploited by a threat or group of threats.

1. Object

The object of this Service Agreement is to define the specific conditions for the supply, by 3DS OUTSCALE, in accordance with SecNumCloud label requirements, of the Service(s) ordered by the CLIENT under the terms of the Agreement.

1. Revision

Any modification of this Service Agreement must be submitted to the CLIENT for acceptance.

1. Termination in the event of loss of certification

It is hereby specified that the Service Agreement may be terminated without penalty, in the event that 3DS OUTSCALE loses its SecNumCloud qualification. If 3DS OUTSCALE loses its certification, it must notify the CLIENT immediately by registered letter with acknowledgment of receipt.

1. The third parties involved in the supply of the Service, their obligations, rights and responsibilities as well as those of 3DS OUTSCALE
2. Data centers

In the framework of the Services, 3DS OUTSCALE will work with the following data centers which have ISO/IEC 27001 certification and are situated in France**:**

|  |  |  |
| --- | --- | --- |
| Name | Address | Services |
| EQUINIX | 110 bis avenue du général Leclerc  93500 Pantin, France | Data center (production site) |
| INTERXION | 1-3 rue du Rateau  93120 La Courneuve | Data center (backup site) |
| TELEHOUSE | 1 rue Pablo Picasso, 78114 Magny-les Hameaux, France | Data center (production site) |

“Data center” Services consist in:

* + The provision of hosting premises for the OUTSCALE Infrastructure
  + the supply of electricity resources
  + the cooling system
  + the fire detection system access control
  + surveillance of premises
  + as well as business continuity and recovery plans for all the obligations mentioned above.

1. Other third parties involved in the supply of the Service.

In the framework of the Services, in addition to the third party “Datacenter”, 3DS OUTSCALE works with the following third parties:

|  |  |  |
| --- | --- | --- |
| Service Provider | Address | Services |
| LUMEN (formerly LEVEL 3/CenturyLink) | * 55 avenue des Champs Pierreux 92000 Nanterre, France | Transit IP |
| COGENT | * 77 boulevard de la République * 92250 La Garenne Colombes | Transit IP |
| SIPARTECH | * 7 rue Auber * 75009 Paris, France | Dark fiber |
| RATPConnect (formerly Telcité) | 6 avenue Montaigne  93160 Noisy-le-Grand, France | Dark fiber |

The “Transit IP” service consists in: dedicated Internet access, HSIP (High Speed Internet Protocol) port and services.

The “Dark fiber” service consists in the supply and maintenance of dark fiber.

1. Obligations, rights and responsibilities of the third parties and of 3DS OUTSCALE

No 3DS OUTSCALE obligation other than those mentioned in (i) and (ii) above exists towards the entities above.

3DS OUTSCALE is responsible for the above third parties’ compliance with its obligations under this Service Agreement in relation to the Services that it entrusts to them.

1. Change of third party involved in the supply of the Service

3DS OUTSCALE shall inform the CLIENT if any change in third party involved in the implementation of the service has an effect on the level of security of the Service.

1. Obligations, rights and responsibilities of the Parties

In addition to the general obligations of the Parties stipulated in the Agreement, the Parties undertake to comply with the following obligations:

1. Location of the Service and the Data/transfer abroad

3DS OUTSCALE undertakes to supply the Service and all the related operations such as Support exclusively within the territory of the European Union.

CLIENT Data, whether personal or not, are hosted in Data centers located in France.

1. Quality of Services/compliance with standards

3DS OUTSCALE will put all of its know-how into carrying out the Services with a view to executing them in accordance with the state of the art and with their Specifications and in line with its ISO/IEC 27001 certification and the SecNumCloud label.

1. Administration, Supervision and Support

Administration, Supervision and Support Services are carried out in France or the European Union.

1. Regionalization

Service interfaces are available in French.

Support may be provided in French or in English, as chosen by the CLIENT when opening the support ticket.

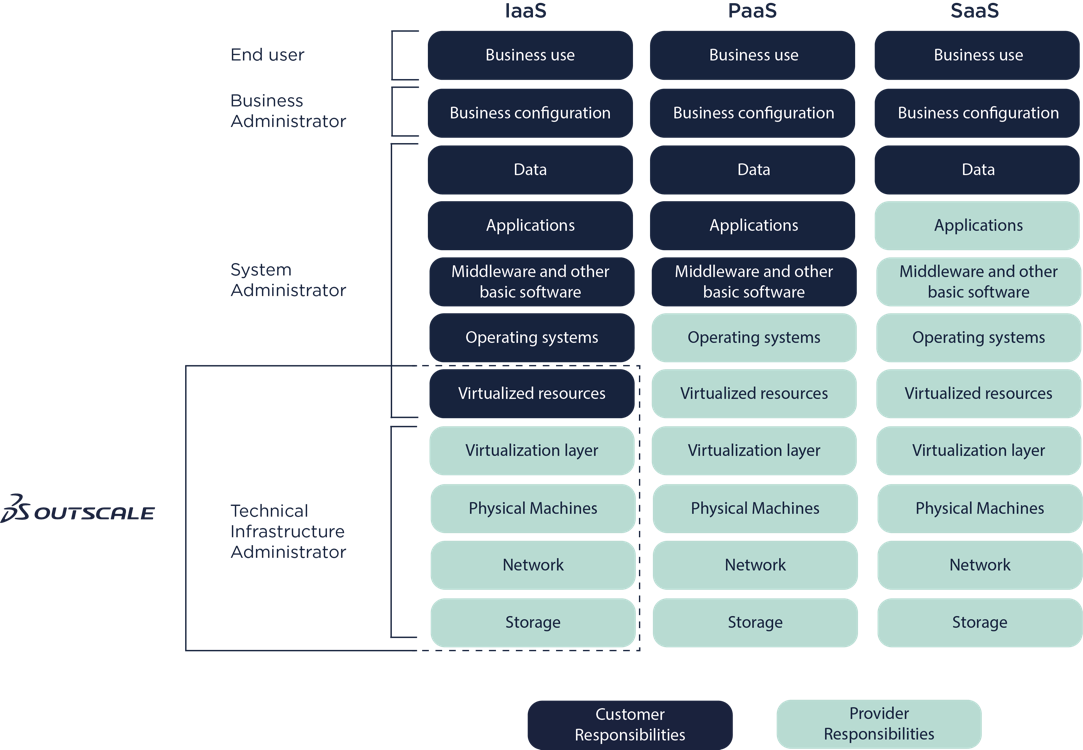
1. 3DS OUTSCALE’s obligations with regard to remote access

Platform Administrators may be required, for standby operations, to access the platform’s Administration network remotely.

The administration workstations used in this framework are dedicated specifically to these Administration operations alone and cannot be used for any other purpose, in accordance with the SecNumClould certification.

1. Elements explicitly excluded from 3DS OUTSCALE’s responsibility

In the framework of this Service Agreement, 3DS OUTSCALE explicitly excludes liability, within the limit of applicable legal and regulatory requirements, in relation to all the elements listed below which are not indicated as being part of the scope of the Services supplied by 3DS OUTSCALE.



1. Responsibility matrix

The matrix below defines the obligations, rights and responsibilities of 3DS OUTSCALE and of the CLIENT which have an impact in the framework of the contractual relations between the CLIENT and 3DS OUTSCALE as part of a Service carried out in application of this Service Agreement and in accordance with the SecNumCloud qualification, without prejudice to the other obligations of the Parties stipulated elsewhere in this Service Agreement. The other obligations, rights and responsibilities of the Parties linked to the SecNumCloud label are available in 3DS OUTSCALE’s applicability statement reference SNC – Applicability statement v51 (the last up-to-date version will be accessible to the CLIENT on demand).

.

The obligations, rights and responsibilities of third parties are indicated in the article “Third parties involved in the supply of the Service, their obligations, rights and responsibilities and those of 3DS OUTSCALE” contained in this Service Agreement.

|  |  |  |
| --- | --- | --- |
| **Reference documents** | **3DS OUTSCALE obligations** | **CLIENT obligations** |
| [**5 – Information security and risk management policies**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711405) | Carry out state-of-the-art services for this type of activity.  Use stable software which has security patch monitoring and which is set up to obtain an optimal level of security.  Apply ANSSI’s guidelines for a healthy information system.  Implement, document, circulate, apply and monitor a security policy that covers:   * – periodical risk assessment * – security of human resources * – asset management * – access control and identity checks * – data encryption * – physical and environmental security * – security linked to operations * - communications security * - surveillance * – running of the technical infrastructure * – management of third parties * – management of incidents linked to information security * – business continuity * – compliance relating to the supply of the service and compliance with national legislation and regulations applicable based on the type of information entrusted.   Undertake to revise its general policy annually as well as following any major change which could have an impact on the service and its assessment of the risks, and have this general policy approved by Management.  Document risk assessment analysis covering the full scope of the service using a method that makes it possible to replicate and compare, taking into account:  - the management of client information with different security needs;  - the risks with an impact on the rights and freedoms of the persons concerned in the event of unauthorized access, unwanted modification and loss of personal data;  - the risks of failure of the technical infrastructure’s resource separation mechanisms (memory, computation, storage, network) shared between clients ;  - the risks linked to the incomplete or non-secure deletion of data stored on memory or storage space shared between clients, in particular during the reallocation of memory and storage space;  - the risks linked to administration interface exposure on a public network. | Ensure that the legal and regulatory requirements applicable to the data entrusted to the Service Provider are respected.  Inform the Service Provider regarding information with specific security needs and pass on the related risk analysis.  Implement a security policy that is not in contradiction with the Service Provider’s security policy. |
| [**6 - Organization of information security**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711409) | Implement an internal security organization and appoint an Information Systems Security Manager, a Physical Security Manager and a Data Protection Officer.  Define and attribute responsibilities in terms of information security for the personnel involved in providing the service.  Conduct and document an assessment of the risks of any project whatsoever that may have an impact on the service.  If a project affects or could affect the level of security of the service, inform the client of the potential impacts and measures implement to mitigate these impacts as well as the related residual risks.  Carry out an impact analysis relating to personal data protection when the processing is likely to generate a risk for the rights and freedoms of the persons concerned. | Define an internal organization to work with the Service Provider on the application of information security. |
| [**7 – Security**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711411) **of human resources** | Implement a process for the verification of personal data in accordance with the laws and regulations applicable and in proportion with the sensitivity of the client information and of the risks identified.  Include a code of ethics in the internal rules and regulations, specifying that:   * – the services are carried out with loyalty, discretion and impartiality; * – the staff involved in supplying the service undertake to: * (i) use methods, tools and techniques that have been validated internally (ii) not to disclose information to a third party, in any form whatsoever, unless formally authorized in writing by the client * (iii) report any illegal content discovered during the service * (iv) comply with applicable national legislation and regulations and good practices linked to their activities * (v) sign the code of ethics.   Provide the client, on demand, with a copy of the code of ethics and the internal rules and regulations of 3DS OUTSCALE.  Set up a training program and ensure that all staff are aware about information security, and provide them with the updated policies and procedures applicable to their assignments.  Establish disciplinary proceedings applicable to staff involved and inform the Client, on demand, of the sanctions applied in the event of a breach of the disciplinary code.  Define and attribute roles and responsibilities relating to the termination, expiration or modification of any contract with a person involved in supplying the service. |  |
| [**8 – Management**](https://wiki.outscale.internal/display/SNC/8+-+Gestion+des+actifs) **of assets** | Keep an inventory of all hardware and software required for the Service and ensure that software licenses are valid throughout the duration of the Service.  Implement a procedure for the return of assets to ensure that each person involved in supplying the service returns all the assets in their possession at the end of their period of employment or contract.  Identify the different information security needs relating to the service.  Implement a procedure for the management of removable media. | Inform the Service Provider if data subject to specific legal, regulatory or sector-based requirements are entrusted to it.  For all data subject to specific requirements, 3DS OUTSCALE requests a preliminary risk analysis. Based on the result of this risk analysis, 3DS OUTSCALE will work with the CLIENT on actions to be taken jointly to provide an adequate response to these risks. |
| [**9 – Access**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711421) **control and identity checks** | Set up and revise annually the access control policy for the Users placed under its responsibility and the Users under the responsibility of the CLIENT, using the account management interface and access rights.  3DS OUTSCALE provides the CLIENT with the means to manage access rights and the identities of the users are the CLIENT’s responsibility.  Keep a list of users and rights attributed and implement the procedures necessary for the attribution, modification and withdrawal of access rights (including withdrawal or suspension) and ensure at the time of attribution of rights that these users do not have access rights that are incompatible and carry out a review of these rights.  Provide separate application program interfaces (API) for its clients.  Set up appropriate separation measures:  (i) between clients;  (ii) between the Service’s information system and the other information systems;  (iii) between the technical infrastructure, the equipment necessary for the administration of the services and the resources hosted.  Revise the list of users within the scope of its responsibility on a quarterly basis.  Implement measures obliging users to sign in to their personal account before being able to access non-nominal technical accounts, where this is necessary.  Implement complexity requirements and renewal mechanisms for client passwords. | Implement means of access control and identity management for users under its responsibility who use account management interfaces and access rights apart from those supplied by the Service Provider.  It is up to the client to define the full set of policies that it wishes to apply to its users and groups of users.  It is the responsibility of the client to review the access rights of its users in relation to the accounts placed at its disposal.  The client logs into the API to manage its account with a request signature.  For every manipulation in its account, the client must sign requests with the secret access key that it has initiated.  3DS OUTSCALE recommends that the CLIENT uses two-factor authentication for the service and imposes use of a code (PIN for an HSM, passwords, …) for certificates allowing access to the service in order to maintain the level of security guaranteed by the SecNumCloud label.  The client is informed that its passwords must be renewed at least every 90 days. |
| [**10 - Cryptology**](https://wiki.outscale.internal/display/SNC/10+-+Cryptologie) | Implement a disc encryption mechanism for use by clients.  Implement the encryption of flows between physical devices.  Implement a password hashing function in line with ANSSI’s rules and recommendations concerning the choice and size of cryptographic mechanisms.  Implement cryptographic keys in line with ANSSI’s rules and recommendations concerning the choice and size of cryptographic mechanisms and protect access to them.  Use a method for the encryption of data and the network stream in line with ANSSI’s rules and recommendations concerning the choice and size of cryptographic mechanisms.  Comply with ANSSI’s rules and recommendations concerning the choice and size of cryptographic mechanisms when using a digital signature mechanism. | Implement encryption of data and flows (via VPN) and data considered “sensitive” following risk assessment procedures. |
| [**11 – Physical**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711436) **and Environmental security** | Implement the means and procedures necessary to guarantee the physical and environmental security of the different areas (public, private and sensitive) involved in the scope of the service, including:   * – limiting and controlling access to protect these areas against unauthorized access, external and environmental threats; * – protecting the electrical and telecommunications wiring.   Guarantee hardware maintenance and implement measures to ensure that installation, repair and maintenance conditions for the information system hardware involved in the service are compatible with confidentiality and uptime requirements.  Implement the means to ensure the level of protection in terms of confidentiality and integrity of outgoing assets, recycled hardware and equipment that has not yet been put into use. |  |
| [**12 – Operating**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711441) **security** | Document operating procedures, keep them up-to-date and make sure they are accessible to the staff concerned.  Implement a procedure for the management of changes and inform the client of all operations that have an impact on security or the availability of the service.  Implement measures to physically separate the development, test and production environments.  Implement measures of protection against malicious codes.  Implement a backup and restoration policy for data under its responsibility and a procedure to test the restoration of backups.  Locate backups at a sufficient distance from the main equipment bearing in mind the risk assessment carried out.  Manage the size of the storage space for all equipment taking into account the evolution of the information system.  Make a log of all events and keep it (for at least 6 months) and protect these elements.  Transfer the logged elements to dedicated servers that are different from the servers that generated the events.  Limit access to the logged events.  Ensure the integrity of the logs over the entire log transmission chain.  Document and implement clock synchronization for all equipment and timestamp each event logged.  Document and implement an infrastructure that makes it possible to analyze and link events recorded by the log system in order to detect events likely to affect the security of the service’s information system with daily analysis alerts.  Implement a procedure to check the installation of software on the service’s information system hardware.  Implement a configuration management procedure for the software environments available for the CLIENT.  Establish a procedure for the management of technical vulnerabilities.  Manage the administration of the Service.  Implement a procedure to oblige 3DS OUTSCALE administrators to use workstations dedicated exclusively to administration tasks. | Analyze and manage risks in relation to virtualized infrastructure deployed on the platform by:   * Providing training for staff authorized to operate the platform, notably regarding the specificities of cloud computing, * Performing regular audits of the backups, data integrity and active user rights on the platform. |
| [**13 – Communications**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711444) **security** | Carry out mapping of the Service’s information system and review it at least once a year.  Implement separation (logical, physical or via encryption) to isolate the network flows and filtering, thus only authorizing legitimate connections. | Analyze and manage the risks in relation to the virtualized infrastructure deployed on the platform by:   * Deploying state-of-the-art resources to limit access to the functional needs established only * Using encrypted and/or dedicated links if necessary for communications deemed sensitive. |
| [**14 - Acquisition, development and maintenance of information systems**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711451) | Implement, document and apply secure development rules for software and systems and train the staff concerned.  Implement and document a procedure to monitor and validate changes before commissioning and keep a version history of software and systems and test them before commissioning.  Implement a secure development environment and run security compliance and functionality tests on upgrades and new elements.  Implement test procedures including the tasks to carry out, the input data and expected output data, ensure the integrity of the pre-production test data.  Request prior authorization from the CLIENT in the event that 3DS OUTSCALE wishes to use its production data to carry out tests and guarantee that the data remains anonymous and confidential. | Implement a procedure to manage the changes made to these systems to manage the impact on data security (availability, integrity, confidentiality, traceability). |
| [**15 - Relations with**](https://wiki.outscale.internal/display/SNC/15+-+Relations+avec+les+tiers) **third partie**[**s**](https://wiki.outscale.internal/display/SNC/15+-+Relations+avec+les+tiers) | Establish a list of third parties involved in the implementation of the Service and demand from these parties:   * – a level of security equivalent to that of 3DS OUTSCALE’s security policy * – audit clauses allowing a certification body to check the application of the “Cloud computing services providers (SecNumCloud) label requirements”, and assess the measures implement on a regular basis * – a review, at least once a year, of the requirements in terms of confidentiality and nondisclosure commitments.   Implement a system for monitoring changes made by third parties, and if the changes are likely to affect the level of security of the service’s information system, inform all clients immediately and take the steps necessary to re-establish the same level of security as before. |  |
| [**16 – Management of incidents linked to information security**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711465) | Define the technical and organizational means necessary to provide a rapid and efficient response to security incidents, and in particular:   * – define response times and means of communications for all the clients concerned, * – inform the staff and the third parties involved in the implementation of the service regarding the incident reporting and management procedure.   Implement a procedure for incident reporting for Clients.  Immediately inform:   * – the clients, regarding security incidents and the related recommendations to limit the impact, and give the clients the possibility of choosing whether to be informed depending on the level of severity of the incidents * – the competent authorities, regarding security incidents   Document the assessment of events and their classification as security incidents and share this information with the Client.  Deal with security incidents until they are solved and inform the Clients concerned; keep proof of security incidents.  Implement a continuous improvement process and draw lessons from incidents linked to information security. | Provide surveillance for hosted components, in particular applications and data, so as to detect any limitation of uptime or violation of data integrity or confidentiality, and process alerts and incidents in accordance with established procedures. These procedures must include informing the Service Provider in the event of alerts or incidents likely to endanger the infrastructure or hosting services. |
| [**17 – Business**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711470) **continuity** | Define the technical and organizational means necessary to ensure business continuity, and in particular:   * – document and implement technical and organizational means and procedures to guarantee compliance with service standards, * – ensure they remain operational, * – restore them, * – test them.   Define internal fail-safe procedures when the hosting service cannot be provided in normal operating conditions (this does not concern the Client’s fail-safe procedures).  Set up a business continuity plan | Implement a business continuity plan for the hosted systems/applications to cope with situations where the hosting service is unavailable for a period that is incompatible with the needs of its own users. The recovery plan must include:   * – its own technical resources (premises, facilities) and procedures to restart the systems/applications in the event of extended unavailability, * – fail-safe modes allowing users to continue their activities in the event of unavailability then resume them when the hosted systems start up again. |
| [**18 - Compliance**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711474) | Implement the means necessary to identify and comply with legal, regulatory and contractual requirements applicable to the service, as well as the specific security needs.  Provide the Client with access to all the procedures relating to this Service Agreement.  Implement periodical control procedures to ensure that the protection measures implemented are in line with the security requirements and policies defined, and fix the rules for these control procedures (type and frequency of testing).  Implement an audit program in line with change management, the policies implemented and the results of risk assessment.  Have an annual audit performed by a certified PASSI (audit of information system security) service provider. | Inform the Service Provider concerning data covered by specific legal, regulatory or sector based requirements.  Implement adequate procedures, in the framework of the use of its services, making it possible to comply with legal, regulatory and contractual requirements in relation to its own client users.  Any transfer of data by the client is under its own responsibility. |

1. Reversibility

In accordance with the Agreement, 3DS OUTSCALE provides the CLIENT with Services in connection with the hosting of data, applications, etc. (the “CLIENT systems” as mentioned in the article “Definitions”).

Reversibility consists in allowing the CLIENT to recover all the elements comprising its Systems (hereafter the “CLIENT elements” or the “Elements”) in order to transfer them to a Service Provider other than 3DS OUTSCALE.

In order to do this, 3DS OUTSCALE places open APIs at the disposal of the CLIENT (or competent third parties designated by the CLIENT) as well as the related documentation, enabling it to recover and transfer the Elements back to its own systems or to a Service Provider other than 3DS OUTSCALE.

For a period of one (1) month following the end of the Service Agreement, 3DS OUTSCALE shall provide the CLIENT with access rights for Reversibility purposes, as explained below.

In the event of the termination of the Service Agreement, for any reason whatsoever, including at the initiative of 3DS OUTSCALE, the CLIENT shall have access to the Platform for **one (1) month** starting from the end date of the Service Agreement, enabling it only to recover all of its Elements.

At the end of this period of **one (1) month**, the CLIENT shall transmit to 3DS OUTSCALE a signed “Recovery of data complete” report. Upon receipt of this report, 3DS OUTSCALE shall end the access necessary to recover the Data and shall delete all CLIENT Data without keeping any trace thereof.

At the end of this period of **one (1) month,** if the CLIENT has not yet sent the signed “Recovery of data complete” report and after formal notice by registered letter with acknowledgment of receipt has been sent to the CLIENT demanding the signed “Recovery of data complete” report but produced no effect after fifteen (15) working days following receipt thereof, 3DS OUTSCALE may invoice the CLIENT for use of the storage space on which the Data are still present for a maximum period of thirteen (13) months. Beyond this, 3DS OUTSCALE reserves the right to delete any remaining Data.

All CLIENT Data will be deleted at the latest two (2) weeks and one (1) day after the end of the Reversibility period.

Furthermore, 3DS OUTSCALE may offer the CLIENT assistance with Reversibility service subject to an order being placed.

1. Data erasure

The secure erasure of all the CLIENT’s Data is performed by 3DS OUTSCALE when the Agreement is terminated or for any other reason.

This erasure is carried out by totally overwriting the storage media on which the data were hosted.

Technical data relating to clients are deleted 90 days after account closing actions.

The CLIENT is provided with a data deletion certificate (**Appendix A**).

1. Service availability/uptime requirements

In accordance with the Agreement, the SLAs are sometimes applicable only on condition that the Client deploys its Systems over all the Availability Zones that exist within the Region. In the case where, although it is possible, the CLIENT decides not to deploy in all the Availability Zones in the Region, it may not request the application of the SLAs. These SLAs are marked with a star (\*).

This limitation concerns neither the APIs provided by 3DS OUTSCALE, nor the Infrastructure set up and hosted by 3DS OUTSCALE which is under the responsibility of 3DS OUTSCALE. For these, the SLAs apply in general, whatever the type of deployment chosen by the Client.

The calculation method for the SLA is described in the specific agreement or in 3DS OUTSCALE’s General Terms and Conditions of Sale.

These guarantees allow 3DS OUTSCALE to commit to the following SLAs on a 24x7 basis.

SLA1 – Service: “Availability of Systems”

* The Individual Availability of a Region is 99.9% per year,
* The Individual Availability of an Availability Zone is 99.7% per year.

SLA2 – Service: “Supply of Cloud Network Services”

The Cloud network is secured in the same way as the Internet network via security groups. The CLIENT is warned that if it decides to bypass the security groups via the Service control API for its internal resources, the configuration of the security groups will NOT be applied.

The latency in the internal network depends on numerous factors, including the proximity of the Availability Zones. Ensuring redundancy in a Region consists in balancing between the geographical distance between the Availability Zones and the maximum latency supported by the Service.

▪Availability of the internal network: **99.99%** per year,

▪Maximum inter-resource latency (excluding Object Storage): **10 ms**,

▪Maximum latency to or from Object Storage: **200 ms**.

SLA3 – Service “Supply of Internet Services (DNS, NTP) and Metadata Cloud Computing Services”

The CLIENT is informed by OUTSCALE that its Systems are protected against intensive use that could lead to denial of service. Any automatic activation of countermeasures due to inappropriate use by the CLIENT leading to the unavailability of the Service for the latter cannot be classified as downtime.

▪Availability of DNS, NTP, DHCP Services: **99.8%** per month

▪Availability of Metadata Services: **99.8%** per month

SLA4 – Service “Secure network supply towards the Internet”

OUTSCALE operates state-of-the-art connections via the Internet. It uses several access providers and BGP-4 Protocol to ensure redundancy. This protocol can lead to sudden changes in route beyond OUTSCALE’s control, but in general this makes it possible to guarantee access availability.

In the event of an incident, the first **2** minutes are never taken into account, because the BGP-4 Protocol convergence time is **90** seconds. The calculation of uptime therefore deducts **2** minutes per incident.

▪Availability of Internet access: **99.999%\*** per year

In the event of a cyberattack, in particular a distributed denial-of-service (DDoS) attack, OUTSCALE may modify its Internet routing configuration to mitigate this attack as far as possible and protect its Infrastructure. If it is a CLIENT IP targeted by the attack, OUTSCALE may use a BGP “blackhole” community to prevent, upstream of the suppliers, any traffic towards the IP under attack in order to protect the CLIENT’s other resources, but also to protect OUTSCALE’s other clients and its Infrastructure.

OUTSCALE incites the CLIENT to do likewise, in particular by using the WAF software available on the market, but also by setting up security groups via the Service Control API. By default, OUTSCALE filters all incoming traffic towards the Client’s public IP addresses and it is the CLIENT who opens the feeds needed. **OUTSCALE insists that the CLIENT restrict flow to a minimum and especially that it does not open SSH (port TCP 22) and RDP (port TCP 3389) administrative flows to the entire Internet (subnet 0.0.0.0/0), as well as internal protocols such as SMB (port TCP/UDP 445) or NFS (port TCP/UDP 2049).**

▪Availability of the Software Firewalls in charge of the security groups: **99.8%\*** per month, ▪Availability of the service Control API Service: **99.9%** per month.

SLA5 – Service “On Demand Load Balancer Service”

▪Availability of the virtual load balancers: **99.78%** per month,

▪Availability of the service control API Service: **99.9%** per month.

SLA6 – Service “Object Storage Service”

▪The Durability of the Storage of an Object in a given Region is **99.9999999999%** guaranteed per year if these objects are distributed throughout the existing Availability Zones within the Region in question,

▪The Availability of the API supplied by OUTSCALE which makes it possible for the CLIENT to publish and manipulate its objects is **99.97%** per year,

▪The Availability of the APIs supplied by OUTSCALE which enable Users to access stored objects is **99.97%** per year for objects deployed in a Region.

Concerning the Object Storage Service, the Durability is subject to state-of-the-art use of the Services and excluding any alteration of data that is deliberate or not stemming from an action carried out by the CLIENT.

The Object Storage Service, like its name implies, must not be used in block mode (for example for an active database). Use of Object Storage in block mode via technical means of circumvention (for example FUSE in Linux), is not a state-of-the-art use of Object Storage and any incident linked to this use will not be covered by this SLA.

SLA7 – Service “Persistent Storage Service”

▪The availability of a volume is **99.7%** guaranteed per month. By default, a volume is only available in its original Availability Zone,

▪The availability of a Snapshot is **99.7%** per month. A Snapshot is available throughout the Region,

▪The Durability of a Snapshot is 99.9999999999%. This Durability is only acquired 24 hours after its creation.

▪For Virtual Machines with guaranteed IPOS persistent storage discs, OUTSCALE undertakes to supply the number of IOPS subscribed within the technical limit per disc and per Virtual Machine, for blocks of 4 ko, at least **90%** of the time over a month.

The Durability of a volume is not guaranteed, because it is a question of storage in active block mode which can be impacted by any unexpected outage problem. For example, one of OUTSCALE’s physical Infrastructure elements crashing may lead to the Virtual Machine resource shutdown and the corruption of a volume of Persistent Storage which has been stopped suddenly in a non-coherent state. In the same way, a “terminate” or “force-stop” order may cause the sudden shutdown of the Virtual Machine resource and may corrupt the attached resource volumes.

The responsibility of OUTSCALE cannot be sought in relation to problems of coherence concerning volumes ; it is up to the CLIENT to ensure that it has made all the backups necessary to perpetuate its data and that it has set up state-of-the-art architecture to be able to recover these volumes in a coherent state.

SLA8 – Service “Non-Persistent Storage”

There is absolutely NO guarantee for the Non-Persistent Storage Service. **OUTSCALE informs the CLIENT that the Service may be interrupted or malfunction at any time,** and that it is the CLIENT’s responsibility to restart its Virtual Machine if this Service breakdown has an impact on its availability.

This Service must only be used in specific cases such as temporary, noncritical storage and certainly not for data such as production data which must be stored on other more durable types of storage medium.

SLA9 – Service “Supply of Virtual Machines on demand”

▪The individual Availability of a hardware resource (bare-metal) belonging to the Infrastructure is **99.7%** per month,

▪The Availability of a Virtual Machine is **99.7%** per month,

▪The Availability of the service control API is **99.9%** per month.

If an element of OUTSCALE’s hardware Infrastructure provokes the shutdown of one of the CLIENT’s Virtual Machines, for example the shutdown of one of OUTSCALE’s physical servers leading to the shutdown of one of the CLIENT’s Virtual Machines, by default the CLIENT’s Virtual Machine is “stopped” to avoid its restart causing additional damage (in particular loss of data, corruption). It is the CLIENT’s responsibility to keep watch over its Virtual Machines and to reboot them if necessary. The time it takes for the CLIENT to do this is not included in the calculation of the Virtual Machine’s downtime.

The time to be counted in the unavailability of a resource is the time during which, following the shutdown of the resource, the CLIENT is unable to restart it.

OUTSCALE informs the CLIENT that in the event of any abnormal use of its Infrastructure, especially in the case of the service control APIs being overloaded (hammering), security countermeasures may be automatically activated and block access to the Service Control APIs or to certain OUTSCALE Services. This does not count as downtime but corresponds to an OUTSCALE Infrastructure backup procedure and the CLIENT may not consider the Service as unavailable.

Lastly, OUTSCALE informs the CLIENT that duplicate requests sent to the APIS are limited to one per second (throttling). If the CLIENT has duplicate requests submitted to the API at a quicker frequency refused on this basis, this does not count as downtime.

SLA10 – Support

Each need or incident must result in the opening of a ticket with OUTSCALE’s Support service. The opening of this ticket with all the information required is the necessary prerequisite and the starting point for assessing compliance by OUTSCALE with its commitments.

The Intervention Time Guarantee covers the time from when the CLIENT opens the support ticket until the first response by the OUTSCALE Support team.

The Recovery Time Guarantee covers the period between the opening of the ticket with all the obligatory information provided by the CLIENT and the resolution of the incident by the OUTSCALE Support team. The CLIENT’s response time in answering a question from the OUTSCALE Support team is deducted from the calculation of the Recovery Time Guarantee period.

An incident that is not noticed by the OUTSCALE Support team can only be measured if the CLIENT submits elements that make it possible to trace an interruption or degradation of service.

Intervention Time Guarantees (GTI) and Recovery Time Guarantees (GTR) are presented below by severity of incident:

|  |  |  |  |
| --- | --- | --- | --- |
| **GTI** | **GTR** | **Incident severity** | **Description** |
| 15 minutes | 2 hours | 1 (Major) | Total and lasting unavailability of a service:  - OOS  - FCU  - API  - Network  - EIM  Excluding programmed maintenance. |
| 30 minutes | 4 hours | 2 (High) | Degradation of service or a service platform:  - OOS  - FCU  - API  - Network  - EIM  - Client portal  - Tools for which a bypass solution exists (example: Cockpit) |
| 1 hour | 48 working hours | 3 (Minor) | Isolated incident, bug or regression, request for analysis of a CLIENT incident. |

For this SLA to apply, the CLIENT must prove that equivalent resources to the defective resource have effectively been deployed in all the Availability Zones in the Region and that despite this 3DS OUTSCALE was unable to re-establish the Service. If the CLIENT resources have been deployed only in one Availability Zone, this SLA does not apply.

1. Service confidentiality requirements

3DS OUTSCALE undertakes not to disclose information relating to the Services to third parties without the formal, written authorization of the CLIENT.

1. CLIENT Data

3DS OUTSCALE is not free to dispose of the Data transmitted and generated by the CLIENT as it chooses; the CLIENT alone has free disposition of its Data.

3DS OUTSCALE cannot claim ownership of the Data transmitted and generated by the CLIENT; the CLIENT alone has full ownership of its Data.

3DS OUTSCALE must seek the prior agreement of the CLIENT before using the CLIENT’s production Data to carry out tests.

Within the framework of technical support, if actions necessary to the diagnosis and the resolution of a problem require an access to the data of the CLIENT, then 3DS OUTSCALE will ask the CLIENT for its consent before intervening.

3DS OUTSCALE’s Services give the CLIENT the possibility of storing and processing its Data exclusively in France or within the European Union.

The CLIENT undertakes to inform 3DS OUTSCALE if it entrusts Data to it that is subject to specific legal, regulatory or sector-based requirements.

All the elements that make up the CLIENT Systems shall remain the property of the CLIENT in all circumstances, this Services Agreement involving no transfer or assignment of intellectual and/or industrial (patent) property rights.

1. Service Compliance

**The Services provided by 3DS OUTSCALE in the framework of this Services Agreement are SecNumCloud certified.**

**A qualification certificate is attached to this Services Agreement (Appendix B). The CLIENT Operations Manager will be notified of any modification or renewal of the certificate which will replace the certificate in Appendix B.**

**The CLIENT can file a complaint concerning the qualified Service with the ANSSI.**

**3DS OUTSCALE commits itself to inform the CLIENT within one month of any legal, organisational or technical change which could have an impact on the conformity of the Service to the requirements of the SecNumCloud referential, in particular concerning the protection with regard to the extra-European law.**

1. Evaluation and audit

By signing this Service Agreement, the CLIENT authorizes

* ANSSI and the certification organization to evaluate the Service and its Information System and ensure they comply with the SecNumCloud qualification requirements,
* A qualified Information Systems Security Auditor appointed by 3DS OUTSCALE to carry out audits on the security of 3DS OUTSCALE’S Information System,

For its part, 3DS OUTSCALE undertakes to:

* Place at the disposal of the CLIENT, or any third party auditor appointed by the latter, the documentation necessary to prove that it satisfies all the obligations relating to compliance with the provisions of article 28 of the General Data Protection Regulation for the purpose of carrying out audits.

1. Contact persons

Client operations manager:

Name:

Position:

E-mail:

Telephone:

3DS OUTSCALE operations manager:

Name: Gaëtan JEUNET

Position: Chief Operations Officer

E-mail: [support@outscale.com](mailto:support@outscale.com)

Telephone: 0 826 20 63 07 ou +33 1 53 27 52 70

These Contact persons will be notified in the event of changes made to the Service or in the event of incidents.

A change in one of the Parties’ Managers must give rise to a document, in any form whatsoever, signed between the legal representatives of the two Parties.

Furthermore, the CLIENT and 3DS OUTSCALE undertake to provide an up-to-date list of additional contact persons in order to guarantee the smooth execution of the Service Agreement, to be completed in **Appendix C** of this Agreement.

1. Applicable law

Unless there is a contractual provision to the contrary, this Agreement shall be governed by French law.

Compliance with the law applicable to this Service Agreement is guaranteed by compliance with a list of requirements applicable to 3DS OUTSCALE.

The requirements taken into account by 3DS OUTSCALE are as follows:

* Compliance with the legal and regulatory obligations applicable
* Compliance with contractual obligations
* Protection of personal data
* Professional secrecy
* Breach of trust
* The secrecy of private correspondence
* Invasion of privacy
* Fraudulent access or presence in an information system
* The law on confidence in the digital economy and compliance with regulations in terms of cryptographic test procedures
* The law on military programming
* Corporate social responsibility
* Compliance with intellectual property rights
* Collection of elements of proof

This guarantee is provided by the legal department of 3DS OUTSCALE which is in charge of:

1. Legal and regulatory watch, ensuring permanent legal monitoring of the company’s activities following both changes in national, European and international regulations and in case law, also monitoring economic and competition based aspects to inform the company of practices adopted by the other businesses in the sector;
2. Drawing up the contracts issued by 3DS OUTSCALE, reviewing contracts received from third parties and supervising legal negotiations; monitoring contracts, updating them thanks to a “*contract management*” platform where all contracts are archived and, where applicable, implementing alerts.

The watch is carried out by signing up to sites providing information and alerts by topic, based on the list of applicable requirements. The information concerning the different requirements applicable is provided on a monthly basis in the form of a blog or legal watch report. These articles and reports identify the potential impacts for 3DS OUTSCALE. They are then reviewed by members of the 3DS OUTSCALE legal department and action plans and procedures are documented and implemented depending on the requirements applicable and the impacts identified for 3DS OUTSCALE. 3DS OUTSCALE also identifies security measures to be implemented to meet the applicable requirements.

Done in *place* *date* .

|  |  |
| --- | --- |
| **3DS OUTSCALE**  Name: David CHASSAN  Position: Director of Strategy  Signature | **The CLIENT**  Name:  Position:  Signature |

Appendix A – Certificate of data\* destruction template (do not fill out)

**CERTIFICATE OF DATA DESTRUCTION**

3DS OUTSCALE certifies that the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ account data have been destroyed.

The 3DS OUTSCALE support team received an account closure request ticket on “date” and checked that the data (instances, storage volumes, snapshots and objects) have been destroyed.

Once requests for destruction have been submitted via the API, the data are destroyed permanently at the latest 2 weeks and one day after the request on our entire infrastructure (including automatic backups).

Done in:

On:

Name of signatory:

Position:

Signature:

Company stamp

***\*(PS: This is a data destruction certificate template that should not be filled in).***

Appendix B –SecNumCloud. Qualification certificate

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Appendix C – List of Contact Persons

This list of Contact Persons must be completed by the Parties as accurately as possible in order to guarantee the smooth execution of this Agreement.

The Parties undertake to update this list of Contact Persons in the event of changes.

CLIENT Security Department or Information Systems Security Manager:

Information:

Email:

3DS OUTSCALE Security Department or Information Systems Security Manager:

Information: Security Department

Email: [security@outscale.com](mailto:security@outscale.com)

CLIENT Legal Department

Information:

Email:

3DS OUTSCALE Legal Department

Information: Legal Department

Email: legal-fr@outscale.com

CLIENT Compliance Department or DPO

Information:

Email:

3DS OUTSCALE Compliance Department or DPO

Information: DPO

Email: [donnees-personnelles@outscale.com](mailto:donnees-personnelles@outscale.com)

CLIENT Sales Department

Information:

Email:

3DS OUTSCALE Sales Department

Information: Sales Department

Email: [sales-eu@outscale.com](mailto:sales-eu@outscale.com)