**CONVENTION DE SERVICE SECNUMCLOUD**

**ENTRE LES SOUSSIGNÉES,**

OUTSCALE, Société par Actions Simplifiée au capital de 1 849 930 €, immatriculée registre du commerce et des sociétés de Nanterre sous le n° 527 594 493, dont le siège social est sis 1, rue Royale, 319 Bureaux de la Colline, 92210 Saint Cloud, représentée par David CHASSAN dûment habilité aux fins des présentes en sa qualité de Directeur de la Stratégie,

ci-après dénommé le **« Prestataire »** ou **« 3DS OUTSCALE »,**

**D’UNE PART,**

**ET**

ci-après dénommé le « **CLIENT** » ou le « **COMMANDITAIRE** »,

**D’AUTRE PART.**

3DS OUTSCALE et le CLIENT étant ci-après désignés individuellement la « Partie » et collectivement les « Parties ».

Préambule

3DS OUTSCALE est un Prestataire français de services informatiques en nuage s’appuyant sur des infrastructures situées sur le territoire français. 3DS OUTSCALE propose une série de services IaaS, PaaS et SaaS sécurisés, innovants et flexibles.

L’Agence Nationale de la Sécurité et des Systèmes d’Information (« ANSSI ») a publié le référentiel d’exigences « SecNumCloud » applicable aux prestataires de services informatiques en nuage qui font la démarche de se qualifier.

Ce référentiel permet aux clients qui choisissent des prestataires qualifiés SecNumCloud de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité de sa prestation et sur la confiance que le client peut accorder au prestataire.

Les Parties ont conclu un Contrat constitué des Conditions Générales de Vente et d’Utilisation de 3DS OUTSCALE, complétées par la présente Convention de Service pour la fourniture des Services sur le périmètre de la Région « Secteur Public ».

Par dérogation aux Conditions Générales de Vente et d’Utilisation, en cas de contradiction entre celles-ci et la présente Convention de Service, cette dernière prévaudra.

**Il est précisé que 3DS OUTSCALE est qualifié SecNumCloud par l’Agence Nationale de la Sécurité et des Systèmes d’Information (« ANSSI ») au titre du décret n°2015-350 du 27 mars 2015 pour ses services d’informatique en nuage de type *IaaS – CLOUD ON DEMAND*, une attestation de qualification est annexée à la présente Convention de Service (Annexe B). 3DS OUTSCALE est en mesure de fournir lesdits services IaaS en conformité avec les exigences du référentiel SecNumCloud.**

1. Définitions

Les termes et expressions identifiés par une majuscule dans la présente Convention ont le sens qui leur est donné dans le présent article ou dans le contrat spécifique ou dans les Conditions Générales de Vente et d’Utilisation 3DS Outscale auxquelles se rattache la présente Convention.

À l’effet d’interpréter la présente Convention de Service, les Parties sont convenues des définitions suivantes qui complètent celles du contrat spécifique ou des Conditions Générales de Vente et d’Utilisation 3DS Outscale :

**Actions d’administration :** Ensemble des actions d’installation, de suppression, de modification et de consultation de la configuration d’un système participant au Système d’Information du Service et susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.

**Administrateur :** Utilisateur disposant de droits privilégiés lui permettant de réaliser les tâches qui lui sont attribuées. On distingue les Administrateurs suivants :

* **Administrateur de sécurité :** Administrateur en charge de la configuration de sécurité, notamment de la gestion des droits d’accès des Administrateurs.
* **Administrateur d’infrastructure :** Administrateur en charge de la gestion et du maintien en conditions opérationnelles et en condition de sécurité de l’Infrastructure technique du Service. Il est toujours sous la responsabilité du Prestataire.
* **Administrateur système :** Administrateur des ressources logiques supportées par l’Infrastructure technique du Service. Selon le type d’architecture du Service, l’administration système peut concerner les ressources abstraites (machines virtuelles, réseaux virtuels, etc.), les systèmes d’exploitation, les intergiciels, les logiciels métier, etc.
* **Administrateur métier :** Administrateur en charge de l’administration fonctionnelle au niveau applicatif.

**Audit :** Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure les exigences d’un référentiel sont satisfaites.

**Bien :** Tout élément représentant de la valeur pour le Service.

**Conditions Générales de Vente et d’Utilisation 3DS Outscale :** passées entre 3DS OUTSCALE et son CLIENT pour encadrer les Prestations liées à un Compte CLIENT accessibles à l'adresse <https://fr.outscale.com/cgucgv/>.

**Contrat :** Ensemble contractuel constitué du contrat spécifique ou des Conditions Générales de Vente et d’Utilisation de 3DS OUTSCALE, complétées par la présente Convention de Service pour la fourniture des Services sur le périmètre de la Région « Secteur Public ».

**Convention de Service :** Le présent document pris en application du contrat spécifique ou des Conditions Générales de Vente et d’Utilisation de 3DS Outscale et conformément aux exigences du Référentiel SecNumCloud.

**Cloud computing (informatique en nuage) :** Modèle permettant un accès aisé, généralement à la demande, et au travers d’un réseau, à un ensemble de ressources informatiques partagées et configurables.

**Disponibilité :** Aptitude à rendre accessible et dans les performances attendues un Service conformément aux dispositions prévues aux SLA.

**Durabilité :** Probabilité de non-effacement d’une donnée de manière inopinée (l’effacement pouvant être causé par des phénomènes physiques comme le « bit flip », le dysfonctionnement d’une technologie particulière, le vieillissement des supports de stockage, etc.), par exemple : une durabilité de 99,9999999 % par an signifie que 0,0000001 % au plus des données peut être altérés dans l’année.

**État de l’art :** Ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d’information publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d’information, diffusés par des organismes de référence ou encore d’origine réglementaire.

**Incident lié à la sécurité de l’information :** Un ou plusieurs évènement(s) liés à la sécurité de l’information, indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l’activité de l’organisme ou de menacer la sécurité de l’information.

**Menace :** Cause potentielle d’un incident indésirable pouvant nuire à un système ou à un organisme.

**Mesure de sécurité :** Mesure qui modifie la vraisemblance ou la gravité d’un risque. Elle comprend la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et peut être de nature administrative, technique, managériale ou juridique.

**Pénalités** : pénalités associées aux SLA, telles que prévues en Annexe A des Conditions Générales de Vente 3DS OUTSCALE - « Pénalités associées aux SLA ».

**Politique :** Intentions et orientations d’un organisme telles que formalisées par sa direction.

**Prestataire d’Audit de la Sécurité des Systèmes d’Information :** Organisme réalisant des prestations d’audit de la sécurité des systèmes d’information. Il est dit qualifié si un organisme de qualification a attesté de sa conformité au référentiel d’exigences des prestataires d’audit de la sécurité des systèmes d’information.

**Qualité de Service / SLA :** Les engagements de qualité de service de 3DS OUTSCALE, niveau de disponibilité par exemple, relativement au(x) Service(s).

**Référentiel SecNumCloud** : le référentiel d’exigences des Prestataires de services d’informatique en nuage (SecNumCloud), version 3.1 du 11 juin 2018, publié par l’ANSSI qui s’applique au présent Contrat.

**Responsable 3DS OUTSCALE/CLIENT :** Le représentant de 3DS OUTSCALE et celui du CLIENT dans le cadre du Contrat et de la présente Convention de Service prise en application de lui. Les Responsables doivent avoir les compétences techniques requises et la capacité juridique d’engager leur société : ils sont les destinataires des Notifications émises dans le cadre de la Convention de Service. Les Responsables sont définis à l’article « Contacts » de la présente Convention de Service.

**Ressources virtualisées :** Abstraction des ressources matérielles d’un système (CPU, RAM, etc.) qui sont mises à disposition par l’infrastructure technique.

**Réversibilité :** Les diligences qui doivent être effectuées par 3DS OUTSCALE, et par le CLIENT, en cas de résiliation ou terminaison du Contrat, pour que le CLIENT puisse transférer ses Données, programmes, applications, etc. vers d’autres ressources que celles mises à disposition par 3DS OUTSCALE conformément à l’article « Réversibilité » de la présente Convention de Service.

**Risque :** Effet de l’incertitude sur l’atteinte des objectifs. Il est exprimé en termes de combinaison des conséquences d’un évènement et de sa vraisemblance.

**Sécurité d’un Système d’Information :** Ensemble des moyens techniques et non techniques de protection permettant à un Système d’information d’assurer la disponibilité, l’intégrité et la confidentialité des données, traitées ou transmises, et des services connexes que ces systèmes offrent ou rendent accessibles.

**Service(s) 3DS OUTSCALE ou Service(s) :** Le(s) service(s) IaaS commandés par le CLIENT dans le cadre du Contrat et soumis à la présente Convention de Services prise en application dudit Contrat.

**Supervision :** Surveillance du bon fonctionnement d’un Système d’information ou d’un Service. Elle concerne la collecte de données (mesures, alarmes, etc.) mais elle ne permet pas d’agir sur l’élément surveillé (ce qui relève des tâches d’Administration).

**Support Technique (ou Support) :** Ensemble des actions de diagnostic ayant pour finalité la résolution des problèmes rencontrés par le CLIENT. Les tâches réalisées par les équipes en charge du support relèvent de la supervision. Si la résolution du problème nécessite une action de la part du Prestataire, cette dernière relève dès lors de l’Administration et doit être effectuée dans les conditions idoines.

**Système d’information :** Ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l’information.

**Tiers :** L’ensemble des participants à la mise en œuvre du Service (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance, fournisseurs de climatisation, etc.) listés à l’article 5 de la présente Convention de Service

**Utilisateur :** Toute personne disposant d’un Compte d’Accès Cloud dans le périmètre du Service. Ce terme générique englobe les Utilisateurs finaux et les Administrateurs.

**Utilisateur final :** Personne jouissant *in fine* du Service mis en œuvre. Il peut s’agir du personnel du CLIENT dans le cas d’un service interne, ou de ses propres clients dans le cas d’un service proposé à l’extérieur.

**Vulnérabilité :** Faiblesse d’un bien ou d’une mesure pouvant être exploitée par une menace ou un groupe de menaces.

1. Objet

La présente Convention de Service a pour objet de définir les conditions spécifiques de fourniture, par 3DS OUTSCALE, en conformité avec les exigences du Référentiel SecNumCloud, du ou des Services commandé(s) par le CLIENT aux termes du Contrat.

1. Révision

Toute modification de la présente Convention de Service doit être soumise à l’acceptation du CLIENT.

1. Résiliation en cas de perte de la qualification

Il est précisé que la Convention de Service pourra être résiliée sans pénalité en cas de perte par 3DS OUTSCALE de sa qualification SecNumCloud. Si 3DS OUTSCALE perdait sa qualification SecNumCloud, elle devrait immédiatement le notifier au CLIENT par lettre recommandée avec avis de réception.

1. Les tiers impliqués dans la fourniture du Service, leurs obligations, droits et responsabilités et ceux de 3DS OUTSCALE
2. Datacenters

Dans le cadre des Prestations, 3DS OUTSCALE fera appel aux datacenters suivants qui sont certifiés ISO/IEC 27001 et situés en France métropolitaine **:**

|  |  |  |
| --- | --- | --- |
| Nom | Adresse | Prestations |
| EQUINIX | 110 bis avenue du général Leclerc  93500 Pantin, France | Datacenter (site de production) |
| INTERXION | 1-3 rue du Rateau  93120 La Courneuve | Datacenter (site de sauvegarde) |
| TELEHOUSE | 1 rue Pablo Picasso, 78114 Magny-les Hameaux, France | Datacenter (site de production) |

La Prestation « Datacenter » consiste en :

* + la mise à disposition de locaux d’hébergement pour l’Infrastructure 3DS OUTSCALE
  + la fourniture de ressources électriques
  + le système de refroidissement
  + la détection incendie
  + le contrôle d’accès
  + la surveillance des locaux
  + ainsi que la continuité et la reprise d’activité sur l’ensemble des obligations mentionnées ci-dessus.

1. Autres tiers impliqués dans la fourniture du Service

Dans le cadre des Prestations, en sus des tiers « Datacenter », 3DS OUTSCALE fera appel aux tiers suivants :

|  |  |  |
| --- | --- | --- |
| Nom du tiers | Adresse | Prestations |
| LUMEN (ancienemment 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 | Fibre noire |
| RATPConnect (anciennement Telcité) | 6 avenue Montaigne  93160 Noisy-le-Grand, France | Fibre noire |

La Prestation « Transit IP » consiste en : accès Internet dédié, HSIP (High Speed Internet Protocol) port et services.

La Prestation « Fibre noire » consiste en la fourniture et la maintenance de fibre noire.

1. Obligations, droits et responsabilités des tiers et de 3DS OUTSCALE

Aucune autre obligation de 3DS OUTSCALE que celles mentionnées ci-dessus en (i) et (ii) n’est reportée aux entités ci-dessus.

3DS OUTSCALE est responsable du respect par les tiers ci-dessus de ses obligations découlant de la présente Convention de Service au titre des Prestations qu’elle leur confie.

1. Changement d’un tiers impliqué dans la fourniture du Service

3DS OUTSCALE informera le CLIENT si un changement de tiers participant à la mise en œuvre du Service affecte le niveau de sécurité du Service.

1. Obligations, droits et responsabilités des Parties

En sus des obligations générales des Parties stipulées au Contrat, les Parties s’engagent aux obligations suivantes.

1. Localisation du Service et des Données / transfert à l’étranger

3DS OUTSCALE s’engage à fournir le Service et toutes les opérations associées tel que le Support exclusivement sur le territoire de l’Union européenne.

Les Données du CLIENT, qu’elles soient personnelles ou non, seront hébergées dans des Datacenters situés sur le territoire français.

1. Qualité des Prestations / respect des normes

3DS OUTSCALE apportera tout son savoir-faire aux Prestations en vue de les exécuter conformément aux règles de l’art et à leurs Spécifications et dans le respect de sa certification ISO/IEC 27001 et du Référentiel SecNumCloud.

1. Administration, Supervision et Support

Les Prestations d’Administration, de Supervision et de Support du/des Services sont réalisées depuis la France ou l’Union européenne.

1. Régionalisation

Les interfaces du Service sont disponibles en langue française.

Le Support peut être fourni en français ou en anglais au choix du CLIENT lors de la création de son ticket.

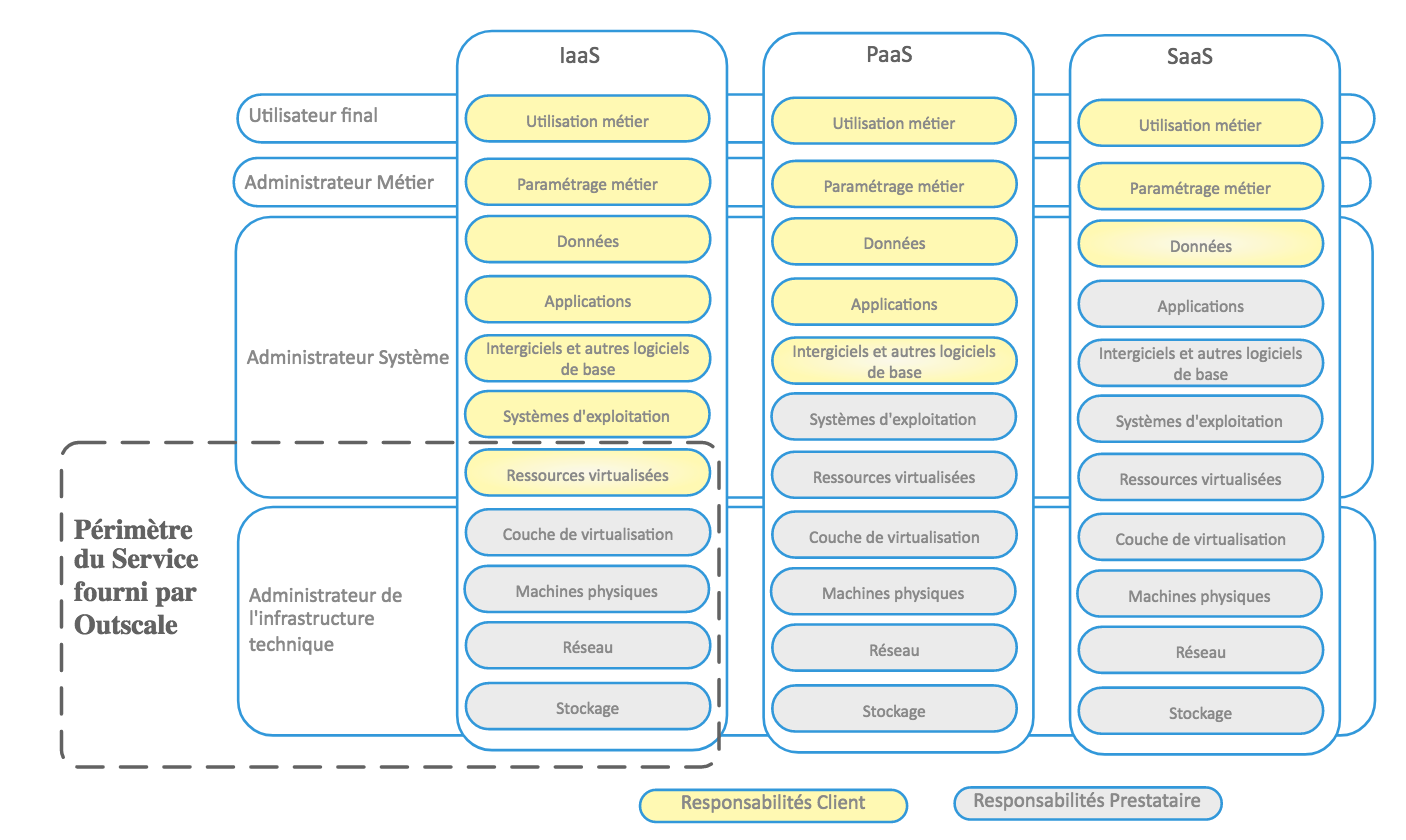
1. Obligations de 3DS OUTSCALE quant aux accès à distance

Les Administrateurs de la plateforme peuvent-être amenés pour des opérations en astreinte à se connecter à distance au réseau d'Administration de la plateforme.

Les postes d'administration utilisés dans ce cadre sont dédiés à ces opérations d'Administration et uniquement à ces opérations et ne peuvent être utilisés pour autre chose en conformité avec le Référentiel SecNumCloud.

1. Éléments explicitement exclus de la responsabilité de 3DS OUTSCALE

Dans le cadre de la présente Convention de Service, 3DS OUTSCALE exclut explicitement toute responsabilité, dans la limite de ce que prévoient les exigences légales et réglementaires en vigueur, sur tous les éléments ci-dessous qui ne sont pas indiqués comme faisant partie du périmètre du Service fourni par 3DS OUTSCALE.



1. Matrice de responsabilité

La matrice ci-dessous définit les obligations, droits et responsabilités de 3DS OUTSCALE et ceux du CLIENT qui ont un impact dans le cadre de la relation contractuelle entre le CLIENT et 3DS OUTSCALE dans le cadre d’un Service rendu en application de la présente Convention de Service et conformément au Référentiel SecNumCloud, sans préjudice des autres obligations des Parties stipulées ailleurs dans la présente Convention de Service. Les autres obligations, droits et responsabilités des Parties liés au Référentiel sont disponibles dans la déclaration d’applicabilité de 3DS OUTSCALE référence SNC – Déclaration d’applicabilité v51 (la dernière version à jour sera accessible à la demande du CLIENT).

.

Les obligations, droits et responsabilités des tiers sont indiqués à l’article « Les Tiers impliqués dans la fourniture du Service, leurs obligations, droits et responsabilités et ceux de 3DS OUTSCALE » de la présente Convention de Service.

|  |  |  |
| --- | --- | --- |
| **Référentiel** | **Obligations de 3DS OUTSCALE** | **Obligations du CLIENT** |
| [**5 - Politiques de sécurité de l'information et gestion du risque**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711405) | Opérer la prestation à l’état de l’art au regard du type d’activité.  Utiliser des logiciels stables bénéficiant d’un suivi des correctifs de sécurité et paramétrés de façon à obtenir un niveau de sécurité optimal.  Appliquer le guide d’hygiène informatique de l’ANSSI au système d’information du service.  Mettre en œuvre, documenter, diffuser, appliquer et contrôler une politique de sécurité couvrant :   * - l'évaluation périodique des risques * - la sécurité des ressources humaines * - la gestion des actifs * - le contrôle des accès et la gestion des identités * - le chiffrement des données * - la sécurité physique et environnementale * - la sécurité liée à l'exploitation * - la sécurité des communications * - la surveillance * - l'exploitation de l'infrastructure technique * - la gestion des tiers * - la gestion des incidents liés à la sécurité de l'information * - la continuité d'activité * - la conformité relative à la fourniture du service et dans le respect de la législation et la réglementation nationale en vigueur selon la nature des informations confiées.   S'engager à réviser annuellement, et à chaque changement majeur pouvant avoir un impact sur le service, sa politique générale et son appréciation des risques et la faire approuver par la Direction.  Documenter une appréciation des risques couvrant l’ensemble du périmètre du service en utilisant une méthode garantissant la reproductibilité et la comparabilité de la démarche en prenant en compte :  - la gestion d’informations client ayant des besoins de sécurité différents ;  - les risques ayant des impacts sur les droits et libertés des personnes concernées en cas d'accès non autorisé, de modification non désirée et de disparition de données à caractère personnel ;  - les risques de défaillance des mécanismes de cloisonnement des ressources de l’infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les clients ;  - les risques liés à l’effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre clients, en particulier lors des réallocations des espaces de mémoire et de stockage ;  - les risques liés à l’exposition des interfaces d’administration sur un réseau public. | S'assurer du respect des contraintes légales et réglementaires applicables aux données qu'il confie au Prestataire.  Communiquer au Prestataire les informations ayant des besoins de sécurité spécifiques et l'analyse de risque associée.  Mettre en œuvre une politique de sécurité qui ne soit pas en contradiction avec la politique de sécurité du Prestataire. |
| [**6 - Organisation de la sécurité de l'information**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711409) | Mettre en œuvre une organisation interne de la sécurité et désigner un Responsable de la Sécurité des Systèmes d'Information, un Responsable de la Sécurité Physique et un Délégué à la Protection des Données.  Définir et attribuer les responsabilités en matière de sécurité de l'information pour le personnel impliqué dans la fourniture du service.  Documenter une estimation des risques préalablement à tout projet, quelle que soit sa nature, pouvant avoir un impact sur le service.  Informer le commanditaire, dans la mesure ou un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, des potentiels impacts et des mesures mises en place pour réduire ces impacts ainsi que les risques résiduels le concernant.  Réalisation d’une analyse d’impact relative à la protection des données à caractère personnel lorsque le traitement est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. | Définir une organisation interne pour collaborer avec le Prestataire dans l'application de la sécurité de l'information. |
| [**7 - Sécurité des ressources humaines**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711411) | Mettre en œuvre une procédure de vérification des informations de son personnel en conformité avec les lois et règlements en vigueur et proportionnellement à la sensibilité des informations du commanditaire et des risques identifiés.  Mettre en place une charte éthique intégrée au règlement intérieur, prévoyant notamment que :   * - les prestations sont réalisées avec loyauté, discrétion et impartialité ; * - les personnels impliqués dans la fourniture du service s'engagent à : * (i) recourir aux méthodes, outils et techniques validés en interne * (ii) ne pas divulguer d'informations à un tiers, sous toutes ces formes, sauf autorisation formelle et écrite du commanditaire * (iii) signaler tout contenu illicite découvert pendant la prestation * (iv) respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités * (v) signer la charte éthique.   Mettre à disposition du commanditaire, s'il le demande, la charte éthique et le règlement intérieur de 3DS OUTSCALE.  Mettre en œuvre un plan de formation et sensibiliser l'ensemble des personnels à la sécurité de l'information, et communiquer les mises à jour des politiques et procédures applicables à leurs missions.  Mettre en place un processus disciplinaire applicable aux personnels impliqués et mettre à disposition du commanditaire, s'il le demande, les sanctions encourues en cas d'infraction.  Définir et attribuer les rôles et responsabilités relatifs à la rupture, au terme ou à la modification de tout contrat avec une personne impliquée dans la fourniture du service. |  |
| [**8 - Gestion des actifs**](https://wiki.outscale.internal/display/SNC/8+-+Gestion+des+actifs) | Tenir à jour un inventaire de l'ensemble des équipements et logiciels mettant en œuvre le Service et s'assurer de la validité des licences tout au long de la Prestation.  Mettre en œuvre une procédure de restitution des actifs permettant de s’assurer que chaque personne impliquée dans la fourniture du service restitue l’ensemble des actifs en sa possession à la fin de sa période d’emploi ou de son contrat.  Identifier les différents besoins de sécurité des informations relatives au service.  Mettre en œuvre une procédure pour la gestion des supports amovibles. | Informer le Prestataire si des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques lui sont confiées  Pour toute donnée soumise à des contraintes spécifiques, 3DS OUTSCALE demande une analyse de risque préliminaire pour ces données. En se basant sur le résultat de cette analyse de risque, 3DS OUTSCALE travaillera avec le CLIENT sur des actions à prendre en commun afin d'apporter une réponse adéquate à ces risques. |
| [**9 - Contrôle d'accès et gestion des identités**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711421) | Mettre en œuvre et réviser annuellement la politique de contrôle d'accès pour les Utilisateurs placés sous sa responsabilité et les Utilisateurs sous la responsabilité du commanditaire utilisant l'interface de gestion des comptes et des droits d'accès.  3DS OUTSCALE fournit les moyens au commanditaire de gérer les droits d'accès et les identités des utilisateurs sont la responsabilité du commanditaire.  Maintenir un inventaire des utilisateurs et des droits attribués et mettre en œuvre les procédures nécessaires notamment pour l'attribution, la modification et le retrait de droits d'accès (incluant la révocation ou la suspension) et s'assurer lors de l'attribution des droits que ces utilisateurs ne possèdent pas de droits d'accès incompatibles entre eux et procéder à une revue des droits.  Fournir des interfaces d'administration distinctes pour ses commanditaires (API).  Mettre en œuvre des mesures de cloisonnement appropriées :  (i) entre les commanditaires ;  (ii) entre le système d’information du service et les autres systèmes d’information ;  (iii) entre l’infrastructure technique, les équipements nécessaires à l’administration des services et les ressources qu’elle héberge.  Réviser trimestriellement la liste des utilisateurs sur son périmètre de responsabilité.  Mettre en place des mesures obligeant les utilisateurs à s’authentifier avec leur compte nominatif avant de pouvoir accéder à des comptes techniques non nominatifs, si ces derniers sont nécessaires.  Mettre en œuvre des règles de complexité et des mécanismes de renouvellement pour les mots de passe client. | Mettre en œuvre les moyens de contrôle d'accès et de gestion des identités pour les utilisateurs sous sa responsabilité qui utilisent des interfaces de gestion des comptes et des droits d'accès hors celles fournies par le Prestataire.  C'est au client de définir l'ensemble des politiques qu'il veut appliquer à ses utilisateurs et ses groupes d'utilisateurs.  Il est de la responsabilité du commanditaire de faire la revue des droits d'accès de ses utilisateurs au sein des comptes mis à sa disposition.  Le client s'authentifie à l'API pour gérer son compte avec une signature des requêtes.  Pour toutes les manipulations au sein de son compte, le client doit signer ses requêtes avec la clé secrète qu'il aura initiée.  3DS OUTSCALE recommande au CLIENT d’utiliser les fonctionnalités de double facteur avec le service et d’imposer l’usage d’un code (PIN sur un HSM, mots de passe, ...) sur ses certificats permettant l’accès au service afin de conserver le niveau de sécurité garantie par la qualification SecNumCloud.  Le client est informé que ses mots de passe doivent être renouvelés à minima tous les 90 jours. |
| [**10 - Cryptologie**](https://wiki.outscale.internal/display/SNC/10+-+Cryptologie) | Mettre en place un mécanisme de chiffrement des disques à disposition des commanditaires.  Mettre en œuvre un chiffrement des flux entre les équipements physiques.  Stocker uniquement l’empreinte des mots de passe des utilisateurs et des comptes techniques.  Mettre en œuvre une fonction de hachage des mots de passe respectant les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de l’ANSSI.  Mettre en œuvre des clés cryptographiques respectant les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de l’ANSSI et en protéger l'accès.  Utiliser une méthode de chiffrement des données, des flux réseau respectant les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de l’ANSSI.  Respecter les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de l’ANSSI lors du recours à un mécanisme de signature électronique. | Mettre en œuvre un chiffrement sur les données et sur les flux (via VPN) et sur les données évaluées comme « sensibles » dans le cadre de l’analyse de risque. |
| [**11 - Sécurité physique et environnementale**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711436) | Mettre en œuvre tous les moyens et procédures nécessaires pour garantir la sécurité physique et environnementale des différentes zones (publiques, privées et sensibles) entrant dans le périmètre du service incluant :   * - la limitation et le contrôle des accès afin de protéger ces zones contre les accès non autorisés, les menaces extérieures et environnementales ; * - la protection du câblage électrique et de télécommunication.   Garantir la maintenance des matériels et mettre en œuvre des mesures permettant de s'assurer que les conditions d'installation, de maintenance et d'entretien des équipements du système d'information du service sont compatibles avec les exigences de confidentialité et de disponibilité.  Mettre en œuvre les moyens permettant de garantir le niveau de protection en confidentialité et en intégrité des actifs sortants, du matériel recyclé et du matériel en attente d'utilisation. |  |
| [**12 - Sécurité liée à l'exploitation**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711441) | Documenter les procédures d’exploitation, les tenir à jour et les rendre accessibles au personnel concerné.  Mettre en œuvre une procédure de gestion des changements et informer le commanditaire de toutes opérations dès lors qu'elles ont un impact sur la sécurité ou la disponibilité du service.  Mettre en œuvre des mesures permettant de séparer physiquement les environnements de développement, de test et de production.  Mettre en œuvre des mesures de protection contre les codes malveillants.  Mettre en œuvre une politique de sauvegarde et de restauration des données qui sont sous sa responsabilité et une procédure permettant de tester la restauration des sauvegardes.  Localiser les sauvegardes à une distance suffisante des équipements principaux au regard de l’analyse de risques réalisée.  Gérer le dimensionnement de l’espace de stockage de l’ensemble des équipements prenant en compte les évolutions du système d’information.  Mettre en œuvre une journalisation des évènements et conserver (au minimum 6 mois) et protéger ces éléments.  Transférer les évènements journalisés sur des serveurs dédiés distincts de ceux qui les ont générés.  Limiter l’accès aux évènements journalisés.  Garantir l’intégrité des journaux sur l’ensemble de la chaîne de transmission des journaux  Documenter et mettre en œuvre une synchronisation des horloges de l’ensemble des équipements ainsi qu’un horodatage de chaque évènement journalisé.  Documenter et mettre en œuvre une infrastructure permettant l’analyse et la corrélation des évènements enregistrés par le système de journalisation pour détecter les évènements susceptibles d’affecter la sécurité du SI du service avec des alarmes quotidiennes d’analyse.  Mettre en œuvre une procédure de contrôle de l’installation de logiciels sur les équipements du SI du service.  Mettre en œuvre une procédure de gestion de la configuration des environnements logiciels disponibles pour le CLIENT.  Mettre en œuvre une gestion des vulnérabilités techniques.  Gérer l’administration du Service  Mettre en œuvre une procédure obligeant les administrateurs de 3DS OUTSCALE à utiliser des terminaux dédiés à la réalisation exclusive des tâches d’administration | Analyser et gérer les risques sur les infrastructures virtualisées déployées sur la plateforme en :   * Assurant la formation des personnes habilitées à exploiter la plateforme, notamment sur les spécificités du cloud * Auditant à intervalle régulier les backups, l'intégrité des données et les accès actifs sur la plateforme |
| [**13 - Sécurité des communications**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711444) | Mettre en œuvre et réviser, a minima annuellement, la cartographie du système d'information du service.  Mettre en œuvre les mesures de cloisonnement (logique, physique ou par chiffrement) pour séparer les différents flux réseau et de filtrage n'autorisant que les connexions légitimes.  Mettre en œuvre une surveillance des réseaux dans le cadre de la détection d'incidents de sécurité | Analyser et gérer les risques sur les infrastructures virtualisées déployées sur la plateforme en :   * Déployant à l'état de l'art les ressources afin de limiter les accès aux seuls besoins fonctionnels établis * Utilisant si nécessaire des liens chiffrés et/ou dédiés pour les communications évaluées comme sensibles |
| [**14 - Acquisition, développement et maintenance des systèmes d'information**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711451) | Mettre en œuvre, documenter et appliquer des règles de développement sécurisé des logiciels et des systèmes, et former les personnels concernés.  Mettre en œuvre et documenter une procédure de contrôle et de validation des changements avant leur mise en production et conserver un historique des versions logicielles et des systèmes et de les tester avant leur mise en production.  Mettre en œuvre un environnement de développement sécurisé et soumettre à des tests de conformité et de fonctionnalité de sécurité les mises à jour et nouveaux éléments du service.  Mettre en œuvre des procédures de tests incluant les tâches à réaliser, les données d'entrée et les résultats attendus en sorties, et d'assurer l'intégrité des données de tests utilisés en préproduction.  Demander l'autorisation préalable au commanditaire dans le cas où 3DS OUTSCALE souhaiterait utiliser des données commanditaires issues de la production pour réaliser des tests et garantir l'anonymisation et la confidentialité des données | Mettre en œuvre une procédure de gestion des changements apportés sur ces systèmes en vue de maîtriser les impacts sur la sécurité des données (disponibilité, intégrité, confidentialité, traçabilité) |
| [**15 - Relations avec les tiers**](https://wiki.outscale.internal/display/SNC/15+-+Relations+avec+les+tiers) | Mettre en place une liste des tiers participants à la mise en œuvre du service, et exiger de ces derniers :   * - un niveau de sécurité équivalent à la politique de sécurité de 3DS OUTSCALE * - des clauses d'audit permettant à un organisme de qualification de vérifier l'application des exigences du référentiel "Prestataires de services d'informatique en nuage (SecNumCloud)", et contrôler régulièrement les mesures mises en place * - une révision, au moins annuellement, des exigences en matière d'engagements de confidentialité ou de non-divulgation d'informations.   Mettre en œuvre un suivi des changements apportés par les tiers, et si les changements sont susceptibles d'affecter le niveau de sécurité du système d'information du service d'en informer sans délai l'ensemble des commanditaires, et mettre en œuvre les mesures nécessaires permettant de rétablir le niveau de sécurité précédent |  |
| [**16 - Gestion des incidents liés à la sécurité de l'information**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711465) | Définir les moyens techniques et organisationnels permettant d'apporter des réponses rapides et efficaces aux incidents de sécurité et notamment :   * - définir les délais et moyens de communication à l'ensemble des commanditaires concernés, * - informer les employés et tiers participant à la mise en œuvre du service de la procédure de gestion des incidents, et des modalités de déclaration des incidents.   Mettre en œuvre une procédure de signalement des incidents pour les commanditaires  Communiquer sans délai :   * - aux commanditaires, les incidents de sécurité et les préconisations associées pour en limiter les impacts, et de donner la possibilité aux commanditaires de choisir d'être notifié en fonction du niveau de gravité des incidents * - aux autorités compétentes, les incidents de sécurité   Documenter l'appréciation des évènements et leur qualification en incident de sécurité, et partager ces informations avec le commanditaire.  Traiter les incidents de sécurité jusqu'à leur résolution et en informer les commanditaires concernés, et garder les éléments de preuve relatifs aux incidents de sécurité.  Mettre en œuvre un processus d'amélioration continu afin de tirer des enseignements des incidents liés à la sécurité de l'information. | Assurer la surveillance des composants hébergés et notamment des applications et des données, de manière à détecter toute atteinte à la disponibilité, à l’intégrité et à la confidentialité des données, et traiter les alertes et incidents selon des procédures définies. Ces procédures doivent prévoir l’information du Prestataire dans le cas d’alertes ou incidents susceptibles de mettre en cause l’infrastructure ou les services d’hébergement. |
| [**17 - Continuité d'activité**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711470) | Définir les moyens techniques et organisationnels permettant d’assurer une continuité de service et notamment :   * - documenter et mettre en place des moyens techniques et organisationnels et des procédures permettant de garantir le respect des engagements de service, * - les maintenir en conditions opérationnelles, * - les restaurer * - les tester   Définir des procédures internes dégradées lorsque le service d’hébergement ne peut pas être assuré comme en fonctionnement nominal (ceci ne concerne pas les procédures dégradées du commanditaire)  Mettre en place un plan de continuité d'activité | Mettre en place un plan de continuité d'activité des systèmes/applications hébergés pour faire face aux situations où le service d’hébergement serait indisponible pour une durée incompatible avec les besoins de ses propres commanditaires. Le plan de reprise doit comprendre :   * - des moyens techniques propres aux commanditaires (locaux, équipements) et des procédures pour redémarrer les systèmes/application en cas d’indisponibilité prolongée, * - des modes dégradés permettant aux utilisateurs de poursuivre les activités en cas d’indisponibilité puis de les reprendre au redémarrage des systèmes hébergés. |
| [**18 - Conformité**](https://wiki.outscale.internal/pages/viewpage.action?pageId=76711474) | Mettre en œuvre les moyens nécessaires permettant d'identifier et de respecter les exigences légales, réglementaires et contractuelles en vigueur applicables au service, ainsi que les besoins de sécurité spécifiques.  Mettre à disposition du commanditaire les procédures relatives à l’ensemble de ses procédures en rapport avec la présente Convention de Service.  Mettre en place des contrôles périodiques visant à̀ s’assurer que les mesures de protection mises en œuvre répondent aux exigences de sécurité et aux politiques de sécurité formalisées, et en définir les règles (nature des contrôles, périodicité.  Mettre en œuvre un programme d'audit en accord avec la gestion du changement, les politiques et les résultats de l'appréciation des risques.  Faire réaliser un audit annuel par un prestataire qualifié PASSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information) | Communiquer au Prestataire les données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques.  Mettre en œuvre les procédures adéquates, dans le cadre de l'utilisation de ses services, permettant de respecter les exigences légales, réglementaires et contractuelles avec ses propres commanditaires.  Le transfert des données par le commanditaire est sous son entière responsabilité. |

1. Réversibilité

Conformément au Contrat, 3DS OUTSCALE met à la disposition du CLIENT des Services permettant l’hébergement de données, d’applications, etc. (les « Systèmes du CLIENT » comme dit à l’article « Définitions »).

La Réversibilité consiste à permettre au CLIENT de récupérer tous les éléments qui composent ses Systèmes (ci-après les « Éléments du CLIENT » ou les « Éléments ») en vue de les transférer chez un autre prestataire que 3DS OUTSCALE.

Pour ce faire, 3DS OUTSCALE met à la disposition du CLIENT (ou des tiers compétents désignés par lui) des API ouvertes, ainsi que la documentation associée, qui lui permettent d’assurer la récupération et le transfert de ses éléments chez lui-même ou un autre prestataire que 3DS OUTSCALE.

3DS OUTSCALE confère, pendant un (1) mois à compter de la fin de la Convention de Service, au CLIENT, un droit d’accès en vue de la Réversibilité, comme expliqué ci-dessous.

En cas de terminaison de la Convention de Service, pour quelque raison que ce soit, y compris à l’initiative de 3DS OUTSCALE, le CLIENT bénéficiera d’un accès à la Plateforme d’**un (1) mois** à compter de la date de la fin de la Convention de Service lui permettant uniquement de récupérer l’ensemble de ses éléments.

À l’issue de ce délai d’**un (1) mois**, le CLIENT transmettra à 3DS OUTSCALE un procès-verbal signé de « Récupération des données terminée ». À compter de la réception de ce procès-verbal, 3DS OUTSCALE mettra fin à l’accès nécessaire à la récupération des Données et effacera toutes les Données du CLIENT et n’en conservera aucune trace.

À partir de ce délai d’**un (1) mois** et si le CLIENT n’a pas adressé de procès-verbal signé de « Récupération des données terminée » et après mise en demeure par lettre recommandée avec avis de réception au CLIENT, d’émettre le procès-verbal signé de « Récupération des données terminée », restée infructueuse pendant les quinze (15) jours ouvrés suivants sa réception, 3DS OUTSCALE pourra facturer l’immobilisation des espaces de stockages sur lesquels les Données sont encore présentes pendant 13 (treize) mois maximum. Au-delà de ce délai, 3DS OUTSCALE se réserve le droit de supprimer les Données dont il est question.

Toutes les données du CLIENT sont effacées au plus tard deux (2) semaines et un (1) jour après la fin de la Réversibilité.

Par ailleurs, 3DS OUTSCALE peut proposer une prestation d’assistance du CLIENT à la Réversibilité soumise à la passation d’un Bon de Commande.

1. Procédure d’effacement

L’effacement sécurisé de l'intégralité des données du Commanditaire est assuré par 3DS OUTSCALE que le Contrat arrive à son terme ou pour toute autre raison.

Cet effacement est réalisé par réécriture complète de tout support ayant hébergé des données.

Les données techniques relatives aux clients sont supprimées 90 jours après les actions de clôture du compte.

Un certificat de suppression des données est fourni au client (**Annexe A**).

1. Exigences de disponibilité du service

Conformément au Contrat, les SLAs ne sont parfois applicables qu’à condition que le CLIENT déploie ses Systèmes sur toutes les Zones de disponibilité qui existent dans la Région. Dans le cas où, alors que c’est possible, le CLIENT décide de ne pas déployer dans toutes les Zones de disponibilité de la Région, il ne pourra pas demander l’application du SLA. Ces SLAs sont marqués d’une étoile (\*).

Cette limitation ne concerne ni les APIs fournies par 3DS OUTSCALE, ni l’Infrastructure mise en place et infogérée par 3DS OUTSCALE et donc de la responsabilité de 3DS OUTSCALE. Pour ces dernières, les SLAs s’appliquent en général, quel que soit le type de déploiement choisi par le CLIENT.

La méthode de calcul des SLA est détaillée dans le contrat spécifique ou dans les Conditions Générales de Vente et d’Utilisation de 3DS Outscale.

Ces garanties permettent à 3DS OUTSCALE de s’engager sur les SLA suivants sur une base 24 h/ 24 et 7 j/ 7 :

SLA1 – Prestation : « domaine de disponibilité »

* La Disponibilité individuelle d’une Région est de 99,9% par an,
* La Disponibilité individuelle d’une Zone de disponibilité est de 99,7% par an.

SLA2 – Prestation : « Service de fourniture réseau intra Cloud»

Le réseau intra Cloud est sécurisé au même titre que le réseau en provenance d’Internet via les groupes de sécurité. Le CLIENT est averti que s’il décide de passer outre les groupes de sécurité via l’API de commande pour ses ressources internes, la configuration des groupes de sécurité ne SERA PAS appliquée.

La latence dans le réseau interne dépend de nombreux paramètres, notamment de la proximité des Zones de disponibilité. La redondance d’une Région est un équilibre entre l’écartement géographique des Zones de disponibilité et la latence maximale supportable par le Service.

▪Disponibilité du réseau interne : **99,99 %** par an,

▪Latence maximale inter ressource (hors Stockage Objet) : **10 ms**, ▪Latence maximale vers ou depuis le Stockage Objet : **200 ms**.

SLA3 – Prestation « Service de fourniture de Services Internet (DNS, NTP) et de Service métadonnées du Cloud Computing »

Le CLIENT est informé par OUTSCALE que ses Systèmes sont protégés contre leur utilisation intensive pouvant mener au déni de service. Toute activation automatique de contre mesure due à une utilisation abusive du CLIENT et entraînant une indisponibilité de Service pour ce dernier ne pourra être comptabilisée comme telle.

▪Disponibilité des Services DNS, NTP, DHCP : **99,8%** par mois

▪Disponibilité des Services métadonnées : **99,8%** par mois

SLA4 – Prestation « Service de fourniture réseau sécurisé vers Internet»

OUTSCALE est à l’état de l’art en ce qui concerne ses connexions via Internet. Il utilise notamment plusieurs fournisseurs d’accès et le protocole BGP4 pour assurer une redondance. Ce protocole peut entraîner des changements de routes intempestifs indépendants de la volonté de OUTSCALE, mais qui en général permettent de garantir une disponibilité de l’accès.

En cas d’incident, les premières **2** minutes ne sont jamais prises en compte, car le temps de convergence du protocole BGP4 est de **90** secondes. Le calcul de disponibilité enlèvera donc **2** minutes par incident.

▪Disponibilité de l’accès Internet : **99,999%\*** par an

En cas de cyber attaque, notamment en cas d’attaque en déni de service distribué (DDoS), OUTSCALE pourra modifier sa configuration de routage Internet pour mitiger au maximum cette attaque et protéger son Infrastructure. Si c’est une IP du CLIENT qui est visée par l’attaque, OUTSCALE pourra utiliser la communauté BGP de type « blackhole » pour interdire en amont de ses fournisseurs tout trafic vers l’IP attaquée afin de protéger les autres ressources du CLIENT, mais aussi des autres clients de OUTSCALE ainsi que son Infrastructure.

OUTSCALE incite le CLIENT à faire de même, notamment en utilisant des logiciels WAF du marché, mais aussi via la configuration des groupes de sécurité via l’API de commande. OUTSCALE par défaut filtre tout trafic entrant vers les IPs publiques du CLIENT et c’est le CLIENT qui ouvre les flux dont il a besoin. **OUTSCALE insiste pour que le CLIENT ouvre ses flux *a minima* et notamment n’ouvre pas les flux d’administration SSH (port TCP 22) et RDP (port TCP 3389) à l’ensemble de l’Internet (subnet 0.0.0.0/0), ainsi que les protocoles internes comme SMB (port TCP/UDP 445) ou NFS (port TCP/UDP 2049).**

▪Disponibilité des Firewalls Logiques en charge des groupes de sécurité : **99,8%\*** par mois, ▪Disponibilité du Service d’API de commande : **99,9%** par mois.

SLA5 – Prestation « Service de répartition de charge à la demande »

▪Disponibilité des load balancers virtuels : **99,78%** par mois,

▪Disponibilité du Service d’API de commande : **99,9%** par mois.

SLA6 – Prestation « Service de Stockage Objets »

▪La Durabilité du Stockage d’un Objet sur une Région considérée est garantie à **99,9999999999%** par an si ces objets sont distribués sur l’ensemble des Zones de disponibilité qui existent dans la Région considérée,

▪La Disponibilité de l’API fournie par OUTSCALE et permettant de publier et manipuler les objets du CLIENT par ce dernier est de **99,97%** par an,

▪La Disponibilité des APIs fournies par OUTSCALE et permettant aux Utilisateurs d’accéder aux objets stockés est de **99,97%** par an pour les objets déployés sur une Région.

Concernant l’offre Stockage Objet, la Durabilité s’entend sous réserve d’une utilisation dans l’état de l’art des Prestations et en dehors de toute altération de données volontaire ou non ayant pour origine une action du CLIENT.

Le Service Stockage Objet , comme son nom l’indique, ne doit pas être utilisé en mode bloc (par exemple pour une base de données en activité). L’utilisation d’un Stockage Objet en mode bloc via des moyens techniques de contournement (par exemple FUSE sous Linux), n’est pas une utilisation dans l’état de l’art du Stockage Objet et tout incident lié à cette utilisation ne sera pas couverte par le présent SLA.

SLA7 – Prestation « Service de Stockage Persistant »

▪La disponibilité d’un volume est garantie à **99,7%** par mois. Par défaut un volume n’est disponible que sur sa Zone de disponibilité d’origine,

▪La disponibilité d’un Snapshot est de **99,7%** par mois. Un Snapshot est disponible sur toute la Région,

▪La Durabilité d’un Snapshot est de 99,9999999999%. Cette Durabilité n’est acquise que 24h après sa création.

▪Pour les Machines Virtuelles possédant des disques de stockage persistant à IOPS garantie attachés, OUTSCALE s’engage à fournir le nombre d’IOPS souscrits dans la limite technique par disque et par Machine Virtuelle, pour des blocs de 4 ko, au moins **90%** du temps sur un mois.

La Durabilité d’un volume n’est pas garantie, car c’est un stockage en mode bloc actif qui peut être impacté par tout problème d’arrêt de service impromptu. Par exemple, le crash d’un élément physique de l’Infrastructure de OUTSCALE peut entraîner l’arrêt d’une ressource type Machine Virtuelle et la corruption d’un volume de Stockage Persistant qui a été brutalement arrêté dans un état non cohérent. De même, une commande « terminate » ou « force-stop », peut causer l’arrêt brutal de la ressource Machine Virtuelle et donc corrompre les ressources volumes attachées.

La responsabilité de OUTSCALE ne peut jamais être engagée sur les problèmes de cohérence concernant les volumes ; c’est au CLIENT de s’assurer qu’il a bien réalisé toutes les sauvegardes nécessaires afin de pérenniser ses données et qu’il a mis en place des architectures à l’état de l’art pour pouvoir retrouver un état cohérent de ses volumes.

SLA8 – Prestation « Service de Stockage Non Persistant»

Le Service de Stockage Non Persistant ne dispose d’absolument AUCUNE garantie. **OUTSCALE informe le CLIENT que le Service peut s’arrêter ou dysfonctionner à tout moment**, et que c’est au CLIENT de redémarrer sa ressource Machine Virtuelle dans le cas où le défaut de ce Service a un impact sur sa disponibilité.

Ce Service ne doit être utilisé que pour des cas précis comme emplacement de stockage temporaire et non critique et surtout pas pour des données comme celles de production à conserver qui doivent être stockées sur d’autres types de stockage plus durable.

SLA9 – Prestation « Service de fourniture de Machines Virtuelles à la carte »

▪La Disponibilité individuelle d’une ressource matérielle (bare-metal) de l’Infrastructure est de **99,7%** par mois, ▪La Disponibilité d’une Machine Virtuelle est de **99,7%** par mois,

▪La Disponibilité du Service d’API de commande est de **99,9%** par mois.

Dans le cas où une ressource matériel de l’Infrastructure de OUTSCALE provoque l’arrêt d’une Machine Virtuelle du CLIENT, par exemple l’arrêt d’un serveur physique de OUTSCALE provoquant l’arrêt d’une Machine Virtuelle du CLIENT, par défaut la Machine Virtuelle du CLIENT est dans un état « stoppé » afin d’éviter que son redémarrage ne provoque des dégâts supplémentaires (notamment perte de données, corruption)Il est de la responsabilité du CLIENT de superviser ses Machines Virtuelles et de les redémarrer si besoin. Le temps nécessaire au CLIENT pour réaliser cela ne rentre pas dans le calcul de l’indisponibilité d’une Machine Virtuelle.

Le temps à comptabiliser dans l’indisponibilité d’une ressource est le temps pendant lequel, suite à l’arrêt de la ressource, le CLIENT est dans l’impossibilité de la redémarrer.

OUTSCALE informe le CLIENT que toute utilisation anormale de son Infrastructure et notamment en cas de surcharge de ses APIs de commande (hammering), des contre-mesures de sécurité pourront s’activer automatiquement et bloquer l’accès aux APIs de commande ou à certaines Prestations OUTSCALE. Dans ce cas, il ne s’agit pas d’une indisponibilité, mais d’une procédure de sauvegarde de l’Infrastructure de OUTSCALE, et le CLIENT ne pourra comptabiliser cela en indisponibilité.

Enfin OUTSCALE informe le CLIENT que les requêtes parfaitement identiques (duplicate) vers ses API sont limitées à une par seconde (Throttling). Le fait que le CLIENT verrait des requêtes identiques présentées à l’API à une fréquence supérieure et refusées à ce titre, ne saurait être comptabilisé en indisponibilité.

SLA10 – Support

Chaque besoin ou incident doit faire l’objet de la création d’un ticket auprès du support OUTSCALE. L’ouverture de ce ticket avec l’ensemble des informations requises est le préalable nécessaire et le point de départ pour évaluer le respect des engagements de OUTSCALE.

Le calcul du délai de la Garantie de Temps d’Intervention (GTI) est la différence entre l’horaire d’ouverture du ticket par le CLIENT et la première réponse du support OUTSCALE.

Le calcul du délai de la Garantie de Temps de Rétablissement (GTR) est mesuré entre l’ouverture du ticket avec l’ensemble des informations obligatoires à fournir par le CLIENT et la résolution de l’incident par le support OUTSCALE. Le temps de réponse du CLIENT pour répondre à une question du support OUTSCALE est déduit du calcul du délai de la Garantie de Temps de Rétablissement (GTR).

Un incident qui n’est pas constaté par l’équipe support OUTSCALE ne peut être mesuré que si le CLIENT apporte les éléments permettant de tracer une coupure ou une dégradation de service.

Les Garanties de Temps d’Intervention (GTI) et les Garanties de Temps de Rétablissement (GTR)sont détaillées ci-dessous par sévérité d’incident :

|  |  |  |  |
| --- | --- | --- | --- |
| **GTI** | **GTR** | **Sévérité Incident** | **Description** |
| 15 minutes | 2 heures | 1 (Majeure) | Indisponibilité totale et durable d'un service :  - OOS  - FCU  - API  - Réseau  - EIM  Hors maintenance programmée. |
| 30 minutes | 4 heures | 2 (Élevée) | Dégradation d’un service ou de la performance d'un service :  - OOS  - FCU  - API  - Réseau  - EIM  - Portail client  - Outils pour lesquels une solution de contournement existe (exemple : Cockpit) |
| 1 heure | 48 heures ouvrées | 3 (Mineure) | Incident isolé, bug ou régression, demande d'analyse sur un incident CLIENT. |

Pour que ce SLA s’applique, il faut que le CLIENT prouve que des ressources équivalentes à la ressource en défaut ont bien été déployées sur toutes les Zones de disponibilité de la Région et que le Service n’a malgré tout pas pu être rétabli par 3DS OUTSCALE. Dans le cas où les ressources du CLIENT n'ont été déployées que sur une seule Zone de disponibilité, ce SLA ne s'appliquera pas.

1. Exigences de confidentialité du service

3DS OUTSCALE s’engage à ne pas divulguer d’informations relatives à la prestation à des tiers, sans l’autorisation formelle et écrite du CLIENT.

1. Données du CLIENT

3DS OUTSCALE ne peut disposer des Données transmises et générées par le CLIENT, leur disposition étant réservée au CLIENT.

3DS OUTSCALE ne peut se prévaloir de la propriété des Données transmises et générées par le CLIENT, ces Données relèvent de la propriété du CLIENT.

3DS OUTSCALE demandera l’accord préalable du CLIENT pour utiliser des Données du CLIENT issues de la production pour réaliser des tests.

Dans le cadre de support technique, si des actions nécessaires au diagnostic et à la résolution d’un problème nécessitent un accès aux données du CLIENT, alors 3DS OUTSCALE demandera préalablement au client son consentement avant d’intervenir.

Les Prestations d’3DS OUTSCALE donnent au CLIENT la possibilité de stocker et traiter ses Données exclusivement en France ou au sein de l’Union européenne.

Le CLIENT s’engage à informer 3DS OUTSCALE s’il lui confie des Données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques.

L’ensemble des éléments composant les Systèmes du CLIENT et ses Données reste en tout état de cause la propriété du CLIENT, la présente Convention de Service n’emportant aucun transfert ou cession de droits de propriété intellectuelle et/ou industrielle (brevet).

1. Conformité du Service

**Les Services délivrés par 3DS OUTSCALE sous l’empire de la présente Convention de Service sont qualifiés au regard du Référentiel SecNumCloud.**

**Une attestation de qualification est annexée à la présente Convention de Service (Annexe B). Toute modification ou renouvèlement de l’attestation sera notifiée au Responsable des opérations CLIENT et remplacera la présente l’Annexe B.**

**Le commanditaire peut déposer une réclamation relative au service qualifié auprès de l’ANSSI.**

**3DS OUTSCALE s’engage à informer dans un délai d’un mois le commanditaire de tout changement juridique, organisationnel ou technique pouvant avoir un impact sur la conformité de la prestation aux exigences du référentiel notamment concernant la protection vis-à-vis du droit extra-européen.**

1. Évaluation et audit

En signant la présente Convention de Service, le CLIENT autorise :

* L’ANSSI et l’organisme de qualification à procéder à la vérification que le Service et son Système d’Information respectent les exigences du Référentiel SecNumCloud,
* Un prestataire d’Audit de la Sécurité des Systèmes d’Information qualifié et mandaté par 3DS OUTSCALE à procéder à des audits de sécurité du Service sur le Système d’Information de 3DS Outscale,

De son côté, 3DS OUTSCALE s’engage à :

* Mettre à la disposition du CLIENT, ou tout auditeur tiers que ce dernier aurait mandaté, la documentation nécessaire pour démontrer le respect de toutes les obligations relatives à la conformité aux dispositions de l’article 28 du Règlement Général sur la Protection des Données pour permettre la réalisation d’audits.

1. Contacts

Responsable des opérations CLIENT :

Nom :

Fonction :

Email :

Téléphone :

Responsable des opérations 3DS OUTSCALE :

Nom : Gaëtan JEUNET

Fonction : Chief Operations Officer

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

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

Attention, ces contacts seront notifiés en cas de changements apportés au Service ou en cas d’incident.

Un changement de Responsable d’une Partie doit donner lieu à un document, sous quelque forme que ce soit, signé entre les représentants légaux des deux Parties.

De plus, le CLIENT et 3DS OUTSCALE s’engagent à fournir une liste tenue à jour de contacts complémentaires afin de garantir la bonne gestion de la présente Convention à compléter en **Annexe C** de la présente Convention.

1. Droit applicable

À défaut de stipulation contractuelle particulière, le droit applicable est le droit français.

Le respect du droit applicable à la présente Convention de Service est garanti par le respect d’une liste d’exigences applicables à 3DS OUTSCALE.

Les exigences prises en compte par 3DS OUTSCALE sont les suivantes :

* La conformité aux obligations légales et réglementaires applicables
* Le respect des obligations contractuelles
* La protection des données à caractère personnel
* Le secret professionnel
* L’abus de confiance
* Le secret des correspondances privées
* L'atteinte à la vie privée
* L’accès ou le maintien frauduleux à un système d’information
* La loi pour la confiance dans l'économie numérique et le respect de la réglementation en matière de contrôles cryptographiques
* La loi de programmation militaire
* La responsabilité sociétale des entreprises
* Le respect des droits de propriété intellectuelle
* La collecte d'éléments de preuve

Cette garantie est assurée par le service juridique d’3DS OUTSCALE chargé notamment :

1. du suivi de la veille juridique, légale et réglementaire, assurant une veille juridique permanente sur les activités de l'entreprise en suivant à la fois les évolutions des réglementations nationales, européennes et internationales, ainsi que la jurisprudence, assurant également une veille économique et concurrentielle pour informer l'entreprise sur les pratiques des autres entreprises du secteur ;
2. d’élaborer les contrats émis par 3DS OUTSCALE, de revoir les contrats reçus des tiers et de superviser les négociations juridiques et le suivi des contrats par la mise à jour des contrats, grâce à une plateforme de « *contract management* » dans laquelle tous les contrats sont archivés et, le cas échéant, assortis d’alertes.

La veille est réalisée par le biais d'inscriptions à des sites d'informations et d'alertes par thème au regard de la liste des exigences applicables. Les informations concernant les différentes exigences applicables sont détaillées mensuellement sous la forme d’articles de blog ou de bulletins de veille juridique. Ces articles et bulletins identifient les impacts potentiels pour 3DS OUTSCALE. Ils sont ensuite revus par les membres du service juridique d’3DS OUTSCALE et des plans d'actions et des procédures sont documentés et mis en œuvre en fonction des exigences applicables et des impacts identifiés pour 3DS OUTSCALE. 3DS OUTSCALE identifie également les mesures de sécurité à mettre en œuvre pour répondre aux exigences applicables.

|  |  |
| --- | --- |
| **Société 3DS OUTSCALE** | **Le CLIENT** |

Annexe A – Modèle d’attestation de suppression des données\* (ne pas compléter)

**ATTESTATION DE SUPPRESSION DE COMPTE/DONNEES**

3DS OUTSCALE atteste que les données du compte \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ont bien été supprimées.

L’équipe de support 3DS OUTSCALE a reçu le ticket de demande fermeture le « date » et a vérifié que les données (instances, volumes de stockage, snapshots et objets) ont bien été supprimées.

Une fois les requêtes de suppression soumises via l’API, les données sont définitivement supprimées au maximum 2 semaines et un jour après la requête sur l’intégralité de notre infrastructure (incluant les sauvegardes automatiques).

Fait à :

Le :

Nom du signataire :

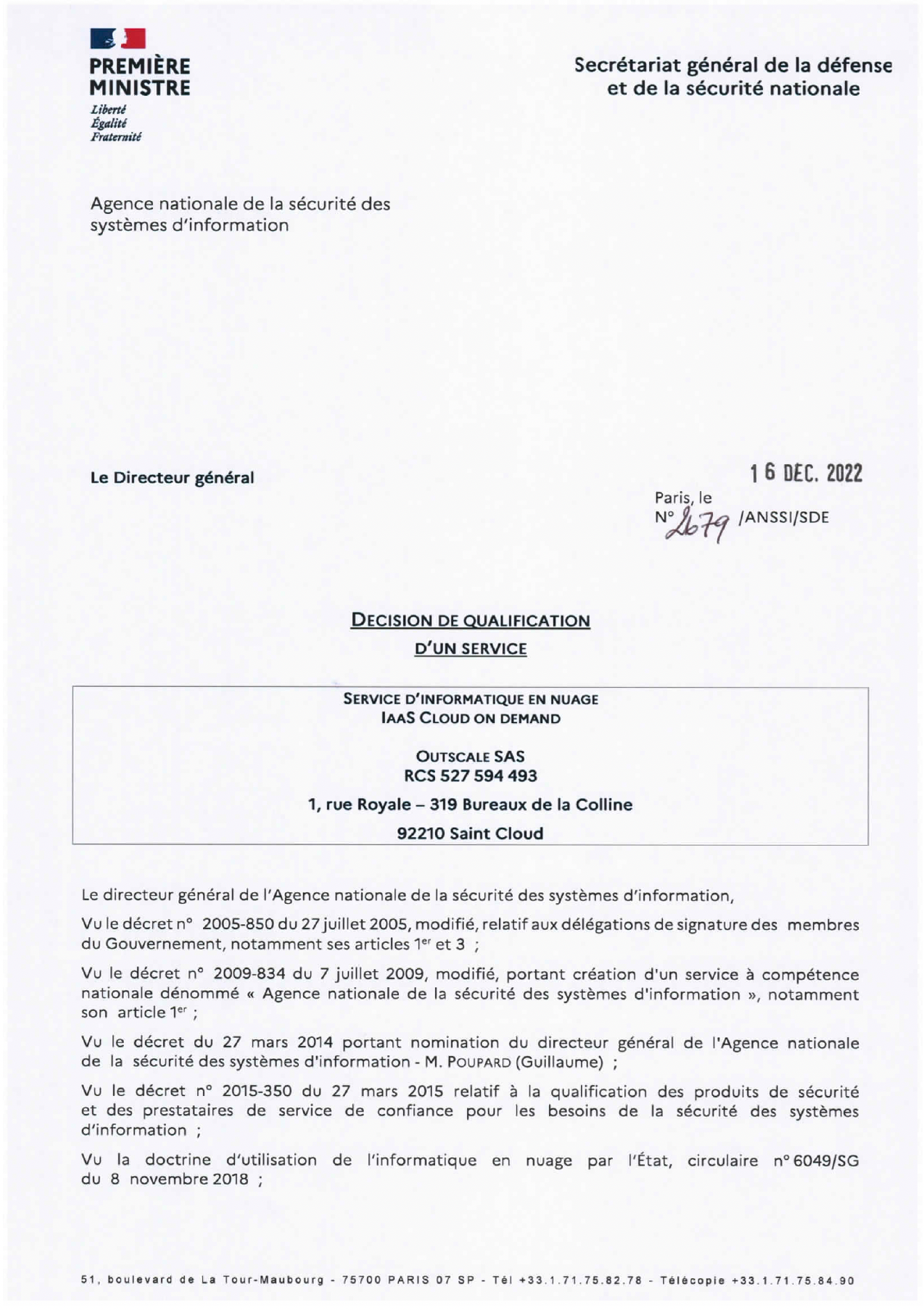
Titre :

Signature :

Cachet de l’entreprise

***\*(PS : Il s’agit d’un modèle d’attestation de suppression des données , il n’est pas nécessaire de le compléter).***

Annexe B – Attestation de qualification SecNumCloud



Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Annexe C – Liste de contacts

Cette liste de contacts est à compléter par les Parties de la manière la plus précise possible afin de garantir la bonne exécution de la présente Convention.

Les Parties s’engagent à mettre à jour cette liste de contacts en cas de changements.

Service Sécurité ou RSSI CLIENT :

Informations :

Email :

Service Sécurité ou RSSI 3DS OUTSCALE :

Informations : Service sécurité

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

Service Juridique CLIENT

Informations :

Email :

Service Juridique 3DS OUTSCALE

Informations : Service juridique

Email : legal-fr@outscale.com

Service Compliance ou DPO CLIENT

Informations :

Email :

Service Compliance ou DPO 3DS OUTSCALE

Informations : DPO

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

Service Commercial CLIENT

Informations :

Email :

Service Commercial 3DS OUTSCALE

Informations : Service commercial

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