Matrice des responsabilités

Table des matières

1. Introduction 2
2. Outillage 2
3. Bonne utilisation du Service 3
4. Régionalisation 4
5. Liste des contacts clients 5
6. Récupération et effacement des données du client / Réversibilité 5
7. Appréciation des risques 7
8. Politique de la sécurité de l'information 8
9. Organisation de la sécurité de l'information 10
10. Sécurité des ressources humaines 11
11. Gestion des équipements 12
12. Contrôle d'accès et gestion des identités 13
13. Cryptographie 16
14. Sécurité physique et environnementale 17
15. Sécurité liée à l'exploitation 18
16. Sécurité des communications 22
17. Sécurité des développements 23
18. Relations avec les fournisseurs 24
19. Gestion des incidents 26
20. Gestion de la continuité d'activité 27
21. Conformité 28

1. Introduction

La matrice des responsabilités est un livrable qui décrit les responsabilités des parties prenantes dans le cadre de leur contractualisation. Les exigences sont en conformité avec les référentiels ISO 27001, HDS et SecNumCloud (SNC).

Les exigences relatives au référentiel ISO 27001 s'appliquent à l'ensemble des Clients ayant signé un contrat avec Outscale.

Les exigences relatives au référentiel SNC s'appliquent uniquement aux Clients ayant signé une convention de service SNC pour les Services qualifiés SNC.

Les exigences relatives au référentiel HDS s'appliquent uniquement aux Clients ayant signé les conditions spécifiques HDS pour les Services certifiés HDS.

Par défaut, tout ce qui s'applique au référentiel ISO 27001 s'applique aux référentiels SecNumCloud et HDS. Les exigences spécifiques relatives aux référentiels SecNumCloud et/ou HDS sont précisées dans la colonne "Référentiel", par termes "SNC" et "HDS" respectivement. Lorsque l'une des responsabilités prévues dans la matrice ne découle d'aucun référentiel, il sera indiqué " - " dans la colonne "Référentiel".

Dans le cas d'utilisation de termes commençant par une majuscule et non définis dans la présente Annexe ni dans le Contrat, il est convenu entre les parties que lesdits termes devront revêtir la même signification que celle prévue dans le référentiel associé.

2. Outillage

- Responsabilité d'Outscale

Description	Référentiel
Outscale fournit au Client une interface d'administration (API ou GUI) de ses Machines Virtuelles pour qu'il puisse y gérer l'infrastructure virtualisée.	-
Outscale fournit une API de commande permettant au Client d'automatiser la gestion et l'administration des Services conformément aux SLA.	-
Dans le cadre des Services, Outscale s'interdit d'accéder aux Données du Client : Outscale gère le stockage physique des Données, mais s'interdit d'accéder à leur stockage logique.	-

- Responsabilité du Client

Description	Référentiel
Il revient au Client, le cas échéant, assisté d'un professionnel de l'informatique, de s'assurer que son Système est administrable via l'interface fournie par Outscale, ce qui implique que le Client aura posé à Outscale toute question utile à cet égard avant d'accepter le Contrat.	-
Le Client utilise les API conformément à leur destination et à la documentation publique (y compris les fonctionnalités de souscription automatique de commandes).	-

3. Bonne utilisation du Service

- Responsabilité d'Outscale

Description	Référentiel
Outscale met à disposition du Client les Services tels que commandés.	-
Outscale fournit les Ressources souscrites On Demand sous réserve qu'elles soient disponibles au moment de la commande.	-
Outscale met à disposition du Client son Service de support au Client via les canaux suivants : - Interface Web de support d'Outscale - Email - Téléphone	-
Outscale n'a pas accès aux Données du Client. Par exception, Outscale pourra accéder aux Données du Client à la demande expresse et écrite de ce dernier et afin de réaliser les actions indispensables au diagnostic et à la résolution d'incident. Outscale pourra refuser toute demande d'intervention impliquant un accès aux Données du Client lorsqu'elle estime l'action réalisable par le Client. En tout état de cause, le support technique est réalisé depuis l'Union Européenne, par du personnel autorisé ayant satisfait aux exigences de recrutement définies par Outscale conformément au référentiel SNC.	SNC – 9.7 d)

- Responsabilité du Client

Description	Référentiel
Le Client s'assure de ne rien faire avec les Services fournis qui puisse mettre en péril les services d'Outscale ainsi que les Ressources des autres Clients.	-
Le Client s'engage à faire un usage raisonnable et de bonne foi des Services mis à sa disposition, et conforme à son activité telle que décrite dans l'expression tacite ou expresse de ses besoins comme à son objet social. Le Client s'interdit en conséquence toute activité qui aurait pour conséquence une utilisation anormale des équipements et matériels nécessaires à la fourniture des Services. Il en est ainsi de toute activité qui aurait pour conséquence une usure prématurée des supports de stockage (notamment les disques durs) mis directement ou indirectement à sa disposition, notamment en pratiquant des activités de calcul, des activités de cryptomining de monnaies virtuelles.	-
Le Client est seul responsable de son Système (y compris les Données, d'où qu'elles viennent) ; il est aussi responsable de ses noms de domaine, certificats SSL, de la gestion des logs de son Système conformément à la loi, etc.	-
Le Client utilise les Services conformément à la documentation publique.	-
Le Client s'assure que le Système n'est pas contraire aux différentes normes, lois, décrets, etc. nationaux et internationaux (incitation à la haine raciale, pédophilie, contrariété à l'ordre public, diffamation, droit de la presse et de la communication audiovisuelle, ordre public économique, spam, criminalité informatique, etc.).	-
Le Client ne doit pas commettre ou faciliter, directement ou indirectement, des actes de contrefaçon, de parasitisme ou de concurrence déloyale au moyen des Services.	-
Si le Client entend opérer des Données critiques ou stratégiques (par exemple, des données de facturation, de paie, des éléments de R&D, etc.) sur les Machines Virtuelles / Stockage	-

Objet Outscale, il revient au Client de souscrire une assurance dédiée à la cybersécurité et aux risques informatiques.	
Dans le cadre de l'utilisation du support, le Client reçoit un numéro de ticket. Le Client doit utiliser ce numéro de ticket dans tous ses échanges avec le support client et conserver l'objet dans tous ses échanges par email afin de permettre un suivi efficace de sa demande et de sa résolution. La procédure détaillée associée au support est décrite dans la Documentation publique Outscale : https://docs.outscale.com	-

4. Régionalisation

- Responsabilité d'Outscale

Description	Référentiel
Outscale fournit à ses clients la documentation associée aux Services et un Service de support en langue française conformément au Contrat.	HDS – 4.5.5
Outscale s'engage à spécifier la liste de l'ensemble des pays au sein desquels les Données du Client sont ou peuvent être hébergées.	HDS – 4.4.7.1 P
Outscale informe le Client des lieux d'hébergement dans lesquels les données de santé seront hébergées.	HDS – 4.4.7.1 C
Outscale permet au Client de choisir les pays d'hébergement dans lesquels les données de santé seront hébergées, et met en œuvre les mesures permettant de respecter ce choix.	HDS – 4.4.7.1 C
Par défaut, Outscale fournira au Client un jeu de Clés d'Accès au Service différent par Région.	-
L'Infrastructure d'Outscale est conçue de manière à ce que la défaillance d'une Zone de disponibilité n'affecte pas toutes les autres Zones de la Région.	-

- Responsabilité du Client

Description	Référentiel
Il est de la responsabilité du Client de lancer son Système sur toutes les Zones de disponibilité d'une Région proposées par Outscale.	-
Lorsque le Client choisit d'héberger des données à caractère personnel de santé, au sens du Règlement général sur la protection des données, il conclut avec Outscale les Conditions particulières HDS et devra choisir parmi les Régions disponibles, le pays d'hébergement dans lequel les données de santé seront hébergées.	HDS – 4.4.7.1 C

5. Liste des contacts clients

- Responsabilité d'Outscale

Référentiel	Référentiel
Outscale conserve la liste des points de contacts désignés par le Client afin de transmettre les coordonnées du contact à l'autorité compétente sur demande. Cette liste est mise à jour régulièrement.	HDS – 4.5.4

- Responsabilité du Client

Description	Référentiel
Le Client s'engage à nommer un Responsable ayant les compétences techniques et la capacité juridique nécessaire pour : - Utiliser et gérer les Services (notamment autoriser et/ou gérer les extensions du périmètre des Services), - Intervenir sur les Ressources, - Gérer le Compte et en particulier s'assurer que les informations de règlement sont toujours valides, afin d'éviter tout retard de paiement. Le Client s'engage auprès d'Outscale à avoir en permanence un interlocuteur Responsable. Ce point de contact doit être en mesure de désigner à Outscale un professionnel de santé lorsque cela est nécessaire.	HDS – 4.5.4

6. Récupération et effacement des données du client / Réversibilité

- Responsabilité d'Outscale

Description	Référentiel
En cas de résiliation du Contrat, pour quelque cause que ce soit, les Données du Client seront effacées comme indiqué ci-dessous, à l'exception des données devant être conservées en vertu de la réglementation en vigueur (notamment les données de facturation et identifications associées seront conservées en raison des obligations légales auxquelles Outscale doit se soumettre pour une durée pouvant aller jusqu'à 10 (dix) ans). La désactivation d'un compte Client est réalisée manuellement par Outscale, mais l'effacement des Données du Client par Outscale est automatique. Dès la désactivation d'un Compte, les données restent accessibles pendant 90 jours avant leur effacement définitif. Une attestation du bon effacement des Données pourra être communiquée au Client s'il en fait la demande à Outscale. Il est précisé au Client que le journal qui constitue la preuve de la suppression des Données du Client est fourni à la demande de ce dernier et est conservé pour une durée d'un (1) an. Le Client dispose donc d'un délai limité pour demander cette preuve. Toutefois, le Client est informé et reconnaît qu'Outscale n'est pas en mesure de procéder à la suppression des Données que le Client aura partagées avec un tiers, notamment par le	-

biais de partage d'OMI ou d'images disques, tant que ce dernier utilise les données partagées. Il appartient au Client de définir les règles de partage de ses Ressources et le cas échéant de ne pas partager d'informations confidentielles et/ou des Données Personnelles. Le Client garantit Outscale et la tiendrait couverte de toute condamnation, quel qu'en soit le fondement, suite à une violation par le Client de cette interdiction.	
Outscale a formalisé une politique encadrant la mise à disposition et la restitution des données à caractère personnel à ses clients, ainsi que leur destruction, et s'engage à la mettre à disposition des clients qui en font la demande.	HDS – 4.4.5.3 P
Outscale a mis en œuvre une procédure de réversibilité définissant les modalités de restitution des données en fin de contrat ou en cas de retrait de sa certification.	HDS – 4.4.5.3 C
Outscale a identifié les données de santé à caractère personnel temporaires et a mis en place les procédures internes nécessaires pour s'assurer de leur effacement.	HDS – 4.4.3.1 P
Outscale garantit que le stockage virtuel alloué au Client ne permet pas de rendre accessible ou visible une donnée précédemment stockée.	HDS – 4.4.6.14

- Responsabilité du Client

Description	Référentiel
Le Client est le seul responsable de son Système et met tout mettre en œuvre pour faciliter les opérations de réversibilité en tant que besoin, ce qui implique notamment, de mettre en place une documentation à cet effet et élaborer des plans de Réversibilité.	-
<u>Récupération de ses Données par le Client s'il a accès à ses Données ;</u> Lorsque le Contrat est résilié, pour quelque raison que ce soit, le Client doit impérativement récupérer toutes ses Données hébergées chez Outscale avant la date de résiliation effective. En effet, à compter de cette date de résiliation effective (à minuit heure de Paris) : (i) le Client n'aura plus accès à ses Données, et (ii) celles-ci seront irrévocablement effacées par Outscale.	-
<u>Récupération de ses Données par le Client s'il n'a pas accès à ses Données :</u> Lorsque le Contrat est résilié, pour quelque raison que ce soit, le Client n'ayant plus accès aux Services en raison d'une suspension des Services, doit impérativement commander à Outscale une Prestation de récupération des Données avant la date de résiliation effective. Le Client ne peut pas commander cette Prestation de récupération de Données s'il n'est pas à jour de ses factures Outscale. Le Client doit donc impérativement régler à Outscale toutes les sommes dont il est débiteur avant la date de résiliation effective. La commande de Prestation de récupération de Données se fait par mail au « Service client » Outscale qui émet un devis. Si le Client accepte le devis, les Données du Client sont récupérées par Outscale, puis transmises au Client dès le paiement du prix de la Prestation de récupération des Données. À compter de la date de résiliation effective (à minuit heure de Paris) les Données du Client seront irrévocablement effacées.	-

7. Appréciation des risques

- Responsabilité d'Outscale

Description	Référentiel
Outscale s'engage à documenter une appréciation des risques couvrant l'ensemble du périmètre du Service.	ISO – 6.1.2 + SNC – 5.3 a)
Outscale réalise son appréciation de risques en utilisant une méthode documentée garantissant la reproductibilité et la comparabilité de la démarche.	ISO – 6.1.2 + SNC – 5.3 b)
Outscale s'engage à prendre en compte dans l'appréciation des risques : - 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'exploitation des interfaces d'administration sur un réseau public ; - les risques d'atteinte à la confidentialité des données des clients par des tiers impliqués dans la fourniture du service (fournisseurs, sous-traitants, etc.) ; - les risques liés aux événements naturels et sinistres physiques ; - les risques liés à la séparation des tâches ; - les risques liés aux environnements de développement.	SNC – 5.3 c)
Outscale s'engage à prendre en compte dans l'appréciation des risques, les exigences légales, réglementaires ou sectorielles spécifiques liées au type d'informations confiées par le client, en s'assurant de respecter les exigences du référentiel SecNumCloud et de ne pas abaisser le niveau de sécurité des exigences du référentiel SecNumCloud.	SNC – 5.3 f) SNC – 8.3 b)
Outscale a identifié les risques associés à des cumuls de responsabilités ou de tâches et les a pris en compte dans l'appréciation des risques et a mis en œuvre des mesures de réduction de ces risques.	SNC – 6.2 a)
Outscale prend en compte dans son évaluation les risques des environnements de développement.	SNC – 14.4 b)
Outscale a défini les mesures nécessaires à la mise en œuvre du traitement des risques et s'assure qu'aucune mesure nécessaire n'a été négligée.	ISO – 6.1.3
Outscale a accepté formellement les risques résiduels identifiés dans son appréciation des risques.	ISO – 6.1.f + SNC – 5.3 e)
Outscale s'engage à réaliser des appréciations des risques de sécurité de l'information à des intervalles planifiés ou quand des changements significatifs sont prévus ou ont lieu.	ISO – 8.2
Outscale s'engage à réviser annuellement son appréciation des risques, et à chaque changement majeur pouvant avoir un impact sur le Service.	SNC – 5.3 f)
Outscale s'engage à analyser et gérer les risques sur les infrastructures virtualisées déployées en : (i) assurant la formation des personnes habilitées à exploiter l'Infrastructure Outscale, notamment sur les spécificités du cloud, (ii) auditant à intervalle régulier les backups, l'intégrité des données et les accès équipements sur l'Infrastructure Outscale, (iii) déployant à l'état de l'art les ressources afin de limiter les accès aux seuls besoins fonctionnels établis, (iv) utilisant si nécessaire des liens chiffrés et/ou dédiés pour les communications évaluées comme sensibles.	-

Outscale s'engage à documenter les risques résiduels liés à l'existence de lois extra-européennes ayant pour objectif la collecte de données ou métadonnées des clients sans leur consentement préalable.	SNC 5.3 d)
Outscale met à disposition du Client, s'il le demande, les éléments d'appréciation des risques liés à la soumission des données du client au droit d'un état non-membre de l'Union Européenne.	SNC-5.3 e) SNC -19.1 e)

- Responsabilité du Client

Description	Référentiel
Pour toute donnée soumise à des contraintes spécifiques, il est de la responsabilité du Client de fournir à Outscale les éléments nécessaires afin d'évaluer si les Services remplissent bien les conditions réglementaires et normatives attendues. En se basant sur ces éléments, Outscale collabore avec le Client sur des actions à prendre en commun afin d'apporter une réponse adéquate.	SNC – 5.3 c) SNC – 8.3 b)
Le Client est responsable de la réalisation des analyses de risques sur le Système.	-

8. Politique de la sécurité de l'information

- Responsabilité d'Outscale

Description	Référentiel
Outscale fournit ses Services dans des conditions conformes à l'état de l'art. Outscale s'efforce d'utiliser des logiciels stables bénéficiant d'un suivi des correctifs de sécurité et paramétrés de façon à obtenir un niveau de sécurité approprié.	ISO + SNC – 5.1 a)
Outscale s'engage à mettre en œuvre une politique de sécurité de l'information adaptée à son contexte d'entreprise et au Service fourni.	ISO – 5.2 + SNC – 5.2 a)
Outscale s'engage à approuver formellement sa politique de sécurité de l'information.	ISO – 5.1.1 + SNC – 5.3 d)
Outscale s'engage à mettre en œuvre un ensemble de politiques de sécurité de l'information diffusé et communiqué à ses employés et aux fournisseurs concernés.	ISO – A5.1.1
Outscale s'engage à appliquer une politique de sécurité couvrant : - L'évaluation périodique des risques ; - La sécurité des ressources humaines ; - La gestion des équipements ; - La 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 ; - Le contrôle de conformité et de suivi ; - L'exploitation de l'infrastructure technique ; - La gestion des fournisseurs ; - La gestion des incidents liés à la sécurité de l'information ; - La continuité d'activité ;	SNC – 5.2 c)

- 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.	
Outscale a identifié, dans sa politique de sécurité de l'information, ses engagements quant au respect de la réglementation qui lui est applicable et à la nature des Données confiées par le Client lorsqu'elle en a connaissance.	SNC – 5.2 b)
Outscale s'engage à revoir les politiques de sécurité de l'information à intervalles programmés ou en cas de changements majeurs.	ISO – A5.1.2
Outscale s'engage à réviser annuellement, et à chaque changement majeur pouvant avoir un impact sur le Service, sa politique générale et son appréciation des risques.	SNC – 5.2 e)
Outscale intègre le guide d'hygiène informatique de l'ANSSI au système d'information à sa politique de la sécurité de l'information.	SNC – 5.1 b)
Outscale définit et attribue les responsabilités en matière de protection de données à caractère personnel en adéquation avec son rôle dans le cadre des traitements concernant le Service, telles que décrites à l'annexe DPA .	SNC - 6.1 e)
Outscale désigne un délégué à la protection des données et s'engage à réaliser et éventuellement contribuer à la réalisation d'une analyse d'impact relative à la protection des données à caractère personnel lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées dans les modalités prévues au DPA.	SNC - 6.1 g) - 6.1h)

- Responsabilité du Client

Description	Référentiel
Pour toute donnée soumise à des contraintes réglementaires spécifiques, il est de la responsabilité du Client de fournir à Outscale les éléments nécessaires afin d'évaluer que les Services remplissent bien les conditions réglementaires et normatives attendues. En se basant sur ces éléments, Les Parties collaborent aux éventuelles actions raisonnables à prendre en commun afin d'apporter une réponse adéquate.	SNC – 5.2 b)
Le Client reconnaît ainsi l'adéquation du Services aux exigences légales et réglementaires applicables à ses Données.	SNC – 5.2 b)

9. Organisation de la sécurité de l'information

- Responsabilité d'Outscale

Description	Référentiel
Outscale s'engage à mettre en œuvre une organisation interne de la sécurité.	ISO – A6.1.1 + SNC 6.1 a)
Outscale a désigné dans son organisation de la sécurité, un responsable du système d'information, un responsable de la sécurité des systèmes de l'information, un responsable de la sécurité physique, un délégué à la protection des données (DPO).	SNC – 6.1 b) e) f) g)
Outscale applique le principe de séparation des tâches et des responsabilités dans son organisation.	ISO – A6.1.2
Outscale a défini et attribué les responsabilités en matière de sécurité de l'information pour le personnel impliqué dans la fourniture du Service, et revoit ses attributions après tout changement majeur pouvant avoir un impact sur le Service.	SNC – 6.1 c) d)
Outscale entretient des relations appropriées avec les autorités compétentes.	ISO – 6.1.3
Outscale entretient des relations appropriées avec des groupes d'intérêt ou des forums spécialisés.	ISO – 6.1.4
Outscale intègre la sécurité de l'information dans la gestion de projet, quel que soit le type de projet.	ISO – 6.1.5
Outscale documente une estimation des risques préalablement à tout projet pouvant avoir un impact sur le Service, et quelle que soit sa nature.	SNC – 6.5 a)
Outscale s'engage à informer le client, dans la mesure ou un projet affecte ou est susceptible d'affecter le niveau de sécurité du Service, des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que les risques résiduels le concernant.	SNC – 6.5 b)
Outscale s'engage à réaliser ou contribuer à la 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.	SNC – 6.1 h)
Outscale a adopté une politique et des mesures de sécurité pour gérer les risques découlant de l'utilisation des appareils mobiles.	ISO – A6.2.1
Outscale a mis en œuvre une politique et des mesures de sécurité pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.	ISO – A6.2.2
Outscale a défini une politique et des mesures pour encadrer les situations de mobilité pour les administrateurs sous sa responsabilité. Dans ce contexte, Outscale s'engage à ce que les mesures mises en œuvre garantissent un niveau de sécurité au moins équivalent au niveau de sécurité hors situation de mobilité.	SNC – 12.12 c)
Outscale met en place des contrôles périodiques visant à 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).	-

- Responsabilité du Client

Description	Référentiel
Outscale recommande au Client de définir une organisation interne pour collaborer avec Outscale dans l'application de la sécurité de l'information.	-

10. Sécurité des ressources humaines

- Responsabilité d'Outscale

Description	Référentiel
Outscale met en œuvre des vérifications, à l'embauche de son personnel, en conformité avec les lois et règlements en vigueur et proportionnellement aux exigences métier, à la sensibilité des informations confiées ainsi qu'aux risques identifiés.	ISO – A7.1.1 + SNC 7.1 a)
Outscale met en œuvre des vérifications renforcées pour les personnels disposant de privilèges d'administration élevés.	SNC 7.1 b)
Outscale met en œuvre pour les salariés et sous-traitants des accords contractuels qui déterminent les responsabilités respectives avec l'organisation en matière de sécurité de l'information.	ISO – A7.1.2
Outscale fait appliquer à tous les salariés et contractants les règles de sécurité définies dans les politiques et procédures en vigueur dans l'organisation.	ISO – A7.2.1
Outscale a mis en place une charte éthique intégrée au règlement intérieur, prévoyant notamment que : - les prestations sont réalisées avec loyauté, discrétion et impartialité et dans des conditions de confidentialité des informations traitées. - les personnels impliqués dans la fourniture du Service s'engagent à recourir aux méthodes, outils et techniques validés en interne, à ne pas divulguer d'informations confidentielles à tout tiers, sous toutes ses formes, sauf autorisation formelle et écrite du client, à signaler tout contenu illicite, à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités, à signer la charte éthique.	SNC – 7.2 a) b)
Outscale met à disposition du client, s'il le demande, la charte éthique et le règlement intérieur d'Outscale.	SNC – 7.2 d)
Outscale met en œuvre des sensibilisations et des formations adaptées pour l'ensemble de ses salariés à la sécurité de l'information et aux risques liés à la protection des données personnelles.	ISO – A7.2.2 SNC – 7.3 a)
Outscale a défini un processus disciplinaire formel et connu de tous pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.	ISO – A7.2.3 SNC – 7.4 a)
Outscale met à disposition du client, s'il le demande, le type de sanctions éventuellement encourues par ses salariés en cas d'infraction des politiques de sécurité.	SNC – 7.4 b)
Outscale a défini et attribué 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.	ISO – A7.3 SNC – 7.5 a)

- Responsabilité du Client

Description	Référentiel
Le Client adresse ses demandes de communication des documents relatifs à la Sécurité des ressources humaines à Outscale via les différents canaux de communication mis à sa disposition (Support, Account Managers ou Service Delivery Manager si applicable).	SNC - 7.4 b) – 7.2 d)

11. Gestion des équipements

- Responsabilité d'Outscale

Description	Référentiel
Outscale identifie et tient à jour un inventaire de l'ensemble des équipements mettant en œuvre le Service.	ISO – 8.1.1 + SNC 8.1 a) b)
Outscale a défini pour chaque actif interne un responsable interne.	ISO – 8.1.2
Outscale s'assure de la validité des licences des logiciels qu'il fournit dans le cadre des Services.	SNC – 8.1 c)
Outscale applique une procédure de restitution des équipements permettant de s'assurer que chaque personne impliquée dans la fourniture du Service restitue l'ensemble des équipements en sa possession à la fin de sa période d'emploi ou de son contrat.	ISO – 8.1.4 SNC – 8.2 a)
Outscale a identifié les différents besoins de sécurité des informations relatives au Service.	SNC – 8.3 a)
Outscale a mis en place une politique de classification de l'information et des procédures de traitement de l'information.	ISO – 8.2
Outscale met en œuvre des procédures pour le marquage et la manipulation de toutes les informations participant à la fourniture du Service.	SNC – 8.4
Outscale s'engage à ce que la destruction des copies papier soit effectuée avec des moyens appropriés.	HDS – 4.4.6.7
Outscale a mis en œuvre des procédures pour la gestion des supports amovibles conformément à sa politique de classification de l'information.	ISO – A8.3 + SNC 8.5 a) b)
Outscale a défini des procédures pour protéger les supports de stockage portables contenant des données à caractère personnel, s'ils sont sortis des locaux, afin que ces données ne soient pas accessibles à du personnel non autorisé.	HDS – 4.4.6.4
Outscale proscrit l'utilisation de supports de stockage portables incompatibles avec des solutions de chiffrement.	HDS – 4.4.6.5
Outscale met en œuvre une politique de sauvegarde, de restauration et de test de restauration des données qui sont (i) sous sa responsabilité, (ii) nécessaires au fonctionnement de la plateforme et (iii) des Snapshots des volumes réalisés par le Client.	ISO - A12.3 SNC - 12.5
Outscale met en œuvre les moyens permettant de garantir le niveau de protection en confidentialité et en intégrité des équipements sortants, du matériel recyclé et du matériel en attente d'utilisation.	SNC - 11.8 SNC - 11.9 SNC - 11.10

- Responsabilité du Client

Description	Référentiel
Il est de la responsabilité du Client d'informer Outscale si des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques lui sont confiées.	SNC – 8.3 b)
Pour toute donnée soumise à des contraintes spécifiques, il est de la responsabilité du Client de fournir à Outscale les éléments nécessaires afin d'évaluer les Services remplissent les conditions réglementaires et normatives attendues. En se basant sur ces éléments, Outscale coopère avec le Client sur des actions à prendre en commun afin d'apporter une réponse adéquate.	SNC – 8.3 b)
Il est de la responsabilité du Client de définir une classification de ses ressources, de les classifier et de sensibiliser ses intervenants dans l'utilisation correcte des ressources mises à sa disposition par Outscale.	-
Le Client doit respecter les termes des licences des logiciels qui lui sont fournis dans le cadre du Service, notamment lorsqu'une licence est nécessaire pour l'utilisation d'un logiciel tiers.	-

12. Contrôle d'accès et gestion des identités

- Responsabilité d'Outscale

Description	Référentiel
Outscale met en œuvre, documente et révise une politique de contrôle d'accès des utilisateurs placés sous sa responsabilité et sur la base d'exigences opérationnelles et de sécurisation de l'information.	ISO – A9.1.1
Outscale s'assure que ces utilisateurs aient uniquement accès au réseau et aux services réseau pour lesquels ils sont autorisés.	ISO – A9.1.2
Outscale met en œuvre une procédure d'enregistrement et de désinscription des utilisateurs et d'accréditation des utilisateurs destinée à permettre l'attribution de droits d'accès.	ISO – A9.2.1 SNC – 9.2 a)
Outscale met en œuvre des processus afin de maîtriser la gestion des accès utilisateur dans l'attribution et la révocation des droits d'accès pour tous les utilisateurs, pour tous les systèmes et tous les Services d'information.	ISO – A9.2.2 SNC – 9.3 a) g)
Outscale met en œuvre des processus afin de restreindre et contrôler l'attribution et l'utilisation des privilèges d'accès.	ISO – A9.2.3
Outscale met en place un processus pour l'attribution des informations secrètes d'authentification.	ISO – A9.2.4
Outscale met en place une revue régulière des droits d'accès des utilisateurs.	ISO – A9.2.5
Outscale s'engage à supprimer ou adapter les droits d'accès de ses utilisateurs à la fin de leur période d'emploi ou en cas de modification de leurs responsabilités.	ISO – A9.2.6
Outscale met en œuvre des règles pour la protection des informations d'authentification et exige que tous ses utilisateurs appliquent ces pratiques.	ISO – A9.3.1
Outscale met en œuvre des restrictions d'accès à l'information et aux applications systèmes.	ISO – A9.4.1
Outscale met en œuvre une procédure de connexion sécurisée pour l'accès aux systèmes et aux applications qui le nécessitent.	ISO – A9.4.2

Outscale met en œuvre des systèmes de gestion des mots de passe qui sont inter équipements et qui garantissent la qualité des mots de passe.	ISO – A9.4.3
Outscale limite et contrôle l'utilisation des programmes utilitaires à privilèges pouvant permettre un contournement des mesures de sécurité.	ISO – A9.4.4
Outscale restreint l'accès aux codes sources des programmes.	ISO – A9.4.5
Outscale fournit les moyens au Client de gérer les droits d'accès et les identités des utilisateurs qui sont de la responsabilité du Client, et la revue des droits.	SNC – 9.3 b) 9.4 b)
Outscale maintient un registre actualisé des utilisateurs ou profils utilisateurs ayant accès aux données à caractère personnel ou aux systèmes utilisés pour leur traitement.	HDS – 4.4.6.9
Outscale met en place des processus afin d'être en mesure de fournir pour un utilisateur donné, sous sa responsabilité ou celle du Client, la liste de tous les droits d'accès sur les différents éléments du système d'information du Service.	SNC – 9.3 e)
Outscale maintient un inventaire des utilisateurs et des droits attribués et met en œuvre les procédures nécessaires notamment pour l'attribution, la modification et le retrait des 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 entres eux et procéder à une revue des droits.	SNC – 9.2 a) c) SNC - 9.3 a) c) d) g)
Outscale attribue des comptes nominatifs lors de l'enregistrement des utilisateurs placés sous sa responsabilité.	SNC – 9.2 b)
Outscale maintient une liste de droits d'accès incompatibles et s'assure lors de l'attribution de droits d'accès que l'utilisateur ne possède pas de droits d'accès incompatibles.	SNC – 9.3 f)
Outscale révise annuellement les droits d'accès des utilisateurs sur son périmètre de responsabilité.	SNC – 9.4 a)
Outscale révise trimestriellement la liste des utilisateurs sur son périmètre de responsabilités.	SNC – 9.4 c)
Outscale déploie des annuaires distincts pour la gestion des comptes utilisateurs placés sous sa responsabilité.	SNC – 9.6 a)
Outscale fournit des interfaces d'administration distinctes pour ses clients.	SNC – 9.6 b) c)
Outscale s'assure que les interfaces d'administration qu'il utilise ne sont pas accessibles à partir d'un réseau public, et ne sont pas utilisables par les utilisateurs du Client.	SNC – 9.6 d)
Outscale met en œuvre des mesures de cloisonnement appropriés : - entre les clients ; - entre le système d'information du Service et les autres systèmes d'information ; - entre l'infrastructure technique, les équipements nécessaires à l'administration des Services et les ressources qu'elle héberge.	SNC – 9.7 a) b) c)
Outscale met en œuvre des procédures de gestion de l'authentification des utilisateurs concernant : - La gestion de moyens d'authentification et leur cycle de vie ; - La mise en œuvre d'authentification à multiples facteurs ; - La vérification de la robustesse des moyens d'authentification.	SNC – 9.5 a)
Outscale met 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.	SNC – 9.5 d)
Outscale met en œuvre des moyens de traçabilité afin de contrôler les actions et les usages des identifiants génériques.	HDS – 4.4.6.8 C

Outscale met en œuvre des mesures afin que les accès aux données à caractère personnel ou aux systèmes utilisés pour leur traitement soit réalisé à l'aide de comptes nominatifs.	HDS – 4.4.6.8 P
Outscale met en œuvre des procédures permettant le blocage d'un compte après un nombre limité de tentatives infructueuses pour les mécanismes d'authentification déployés.	SNC – 9.5 b)

- Responsabilité du Client

Description	Référentiel
Le contrôle d'accès et la gestion des identités des utilisateurs notamment aux Services sont sous la responsabilité du Client. En conséquence, il définit notamment l'ensemble des politiques d'accès aux Services et effectue la revue des droits d'accès des utilisateurs aux Services.	-
Pour toutes les manipulations au sein de son compte, le Client doit authentifier ses requêtes avec les secrets qu'il a initialisés.	-
Outscale recommande au Client d'utiliser les fonctionnalités de double facteur avec le Service et d'imposer l'usage d'un matériel physique distinct afin de conserver le niveau de sécurité garantie par la qualification SecNumCloud.	SNC
Il est recommandé au Client de mettre en place une politique de gestion et renouvellement des mots de passe.	-
Le Client doit régénérer ses Clés d'accès au Service (notamment : mots de passe, etc.) aux Services régulièrement et lorsque Outscale en fait la demande, notamment pour des raisons de sécurité Outscale fournit au Client les outils pour gérer ses politiques d'expiration d'AK/SK. Par ailleurs, si Outscale venait à demander un renouvellement et que le Client ne procède pas à la modification de ses AK/SK dans les meilleurs délais (à savoir dans les VINGT-QUATRE (24) HEURES suivant la demande) la responsabilité d'Outscale quant aux dommages pouvant survenir en lien avec cette absence de modification est écartée.	-
Les Clés d'accès au Service sont sous la garde exclusive du Client.	-

13. Cryptographie

- Responsabilité d'Outscale

Description	Référentiels
Outscale met en œuvre une politique d'utilisation des mesures cryptographiques en vue de protéger l'information.	ISO – A10.1.1
Outscale met en œuvre une politique de gestion des clés cryptographiques.	ISO – 10.1.2
Outscale s'engage à suivre les règles et recommandations de l'ANSSI dans la mise en œuvre des clés cryptographiques.	SNC – 10.5 a) b)
Outscale protège l'accès aux clés cryptographiques et autres secrets utilisés pour le chiffrement des données.	SNC – 10.5 c)
Outscale protège l'accès aux clés cryptographiques et autres secrets utilisés pour les tâches d'administration.	SNC – 10.5 d)
Outscale s'engage à mettre en œuvre un mécanisme de chiffrement empêchant la récupération des données du client en cas de réallocation d'une ressource ou de récupération du support physique.	SNC – 10.1 a)
Outscale s'engage à suivre les règles et recommandations de l'ANSSI concernant le choix et le dimensionnement des mécanismes cryptographiques lors du recours à un mécanisme de signature électronique.	SNC – 10.1 b) c)
Outscale s'engage à mettre en œuvre un chiffrement des données sur les supports amovibles et les supports de sauvegardes qui seraient amenés à quitter le périmètre de sécurité physique du système d'information du Service en question, le cas échéant.	SNC – 10.1 d)
Outscale s'engage à suivre les règles et recommandations de l'ANSSI dans la mise en œuvre des mécanismes de chiffrement des flux réseau.	SNC – 10.2 a) b) c) d) e)
Outscale s'engage à protéger par chiffrement les communications entre site principal et site de sauvegarde.	SNC – 12.5 d)
Outscale ne limite en rien la mise en place autonome d'un chiffrement de disque à la charge du Client.	-
Outscale met en œuvre un chiffrement sur les flux de données et sur les données évaluées comme « sensibles » dans le cadre de l'analyse de risque.	-
Outscale s'engage à ne stocker que l'empreinte des mots de passe des utilisateurs et des comptes techniques.	SNC – 10.3 a)
Outscale s'engage à suivre les règles et recommandations de l'ANSSI dans la mise en œuvre d'une fonction de hachage des mots de passe.	SNC – 10.3 b) c)
Outscale s'engage à suivre les règles et recommandations de l'ANSSI dans la génération des empreintes des mots de passe.	SNC – 10.3 d)
Les API et interfaces d'Outscale sont maintenues conformes à l'état de l'art en matière de cryptographie. Outscale utilise les protocoles suivants : IPSEC, TLS, SSH. De plus, Outscale s'engage à prendre en considération les recommandations faites dans les guides publiés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).	-
Outscale s'engage à suivre les règles et recommandations de l'ANSSI dans la mise en œuvre des mécanismes de signature électroniques.	SNC – 10.4 a) b)
Outscale met 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.	-

Outscale s'engage à utiliser des certificats de clé publique issus d'une autorité de certification d'un État membre de l'Union Européenne	SNC - 10.6.a

- Responsabilité du Client

Description	Référentiel
Outscale recommande au Client de chiffrer ses Données et de ne pas lui remettre la clé de chiffrement. La clé de chiffrement demeure sous la responsabilité du Client.	-

14. Sécurité physique et environnementale

- Responsabilité d'Outscale

Description	Référentiel
Outscale a défini des périmètres de sécurité pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.	ISO – 11.1.1 HDS SNC – 11.1
Outscale a mis en œuvre tous les moyens et procédures nécessaires pour garantir la sécurité physique et environnementale des différentes zones définies (publiques, privées et sensibles) entrant dans le périmètre du Service.	SNC – 11.1
Outscale a mis en œuvre dans ces différentes zones une limitation et un contrôle des accès afin de protéger ces zones contre les accès non autorisés, les menaces extérieures et environnementales.	ISO – 11.1.3 SNC -11.1 a
Outscale s'engage à ce qu'aucune ressource dévolue au Service ou permettant d'accéder à des composants de celui-ci ne soit hébergée dans les zones définies publiques.	SNC – 11.1.1
Outscale s'engage à s'assurer que seul le personnel autorisé est admis dans ces zones.	ISO – A11.1.2
Outscale s'engage à ce que les zones définies privées soient protégées contre les accès non autorisés, et que ce contrôle d'accès physique repose au moins sur un facteur personnel tel que la connaissance d'un secret, la détention d'un objet ou la biométrie.	SNC – 11.2.1 a)
Outscale s'engage à ce que des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents soient appliquées.	ISO – A11.1.4
Outscale a défini et documenté les conditions d'accès physique dérogatoires en cas d'urgence.	SNC – 11.2.1 c)
Outscale a mis en œuvre des procédures pour définir les conditions de réalisation du travail dans les zones sécurisées.	ISO – A11.1.5
Outscale a défini et documenté les plages horaires et conditions d'accès aux zones définies privées en fonction des profils des intervenants.	SNC – 11.2.1 e)
Outscale s'engage à contrôler et limiter l'accès aux zones de livraison, de chargement ou toutes zones dites publiques vers des zones de traitement de l'information, de façon à éviter les accès non autorisés.	ISO – A11.1.6
Outscale a mis en œuvre des moyens pour isoler les points d'accès des zones de livraisons ou de chargement vers les zones définies comme privées et sensibles.	SNC – 11.5

Outscale s'engage à mettre en œuvre les moyens nécessaires pour sécuriser le câblage électrique ou de télécommunication transportant des données ou supportant des services d'information contre toute interception ou tout dommage.	ISO – A11.2.3 SNC 11.6 a)
Outscale s'assure de la maintenance des matériels pour en garantir leur disponibilité et leur intégrité.	ISO – A11.2.4
Outscale met 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.	SNC 11.7 a)
Outscale s'engage à mettre en œuvre les moyens nécessaires pour protéger les matériels afin de réduire les risques liés à des menaces, des dangers environnementaux et des accès non autorisés.	ISO – A11.2.1
Outscale s'engage à mettre en œuvre les moyens nécessaires pour protéger le matériel de coupure de courant et autres perturbations dues à une défaillance des Services généraux.	ISO – A11.2.2
Outscale s'engage à mettre en œuvre des procédures pour gérer la sortie des équipements.	ISO – A11.2.5
Outscale s'engage à mettre en œuvre les moyens permettant de garantir le niveau de protection en confidentialité et en intégrité des équipements sortants, du matériel recyclé et du matériel en attente d'utilisation.	SNC 18.1 a)
Outscale s'engage à mettre en œuvre des mesures de sécurité pour le matériel utilisé hors des locaux.	ISO – A11.2.6
Outscale s'engage à mettre en œuvre des procédures de mise au rebut de tout matériel contenant des supports de stockage.	ISO – A11.2.7
Outscale s'engage à mettre en œuvre des procédures de protection appropriées pour les matériels utilisateurs laissés sans surveillance.	ISO – A11.2.8
Outscale applique une politique du bureau propre et de verrouillage des postes.	ISO – A11.2.9

- Responsabilité du Client

Description	Référentiel
Il est de la responsabilité du Client de définir les mesures physiques et environnementales qui seraient nécessaires et applicables, dans son organisation, pour tout personnel et matériel, dans l'utilisation du Service afin de garantir la sécurité de l'information contre les accès non autorisés, les menaces extérieures et environnementales.	-

15. Sécurité liée à l'exploitation

- Responsabilité d'Outscale

Description	Référentiel
Outscale s'engage à documenter les procédures d'exploitation, les tenir à jour et les rendre accessibles au personnel d'Outscale concerné.	ISO – A12.1.1 SNC – 12.1 a)
Outscale s'engage à contrôler les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information.	ISO – A12.1.2

Outscale s'engage à surveiller et ajuster l'utilisation des ressources et effectuer des projections sur le dimensionnement nécessaire pour garantir les performances exigées du système.	ISO – A12.1.3
Outscale s'engage à séparer les environnements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans les environnements d'exploitation.	ISO – A12.1.4
Outscale s'engage à mettre en œuvre une procédure de gestion des changements et informer le client de toutes opérations dès lors qu'elles ont un impact négatif sur la sécurité ou la disponibilité du Service.	SNC – 12.2 a) b)
Outscale s'engage à mettre en œuvre des mesures permettant de séparer physiquement les environnements de développement, de test et de production.	SNC – 12.3 a)
Outscale s'engage à mettre en œuvre des mesures de protection et de sensibilisation contre les codes malveillants incluant mesures de détection, de prévention et de récupération conjuguées à la sensibilisation adaptée.	ISO – 12.2.1 SNC 12.4 a) b)
Outscale s'engage à mettre en œuvre une politique de sauvegarde et de restauration des données qui sont sous sa responsabilité afin de garantir les SLAs sur la durabilité des snapshots et du stockage objet, et une procédure permettant de tester la restauration des sauvegardes.	ISO – 12.3.1 SNC – 12.5 a) c)
Outscale s'engage à mettre en œuvre des mesures de protection des sauvegardes, de les localiser à une distance suffisante des équipements principaux, et d'y appliquer les mêmes exigences de sécurité que pour le site principal.	SNC – 12.5 b) d)
Outscale a mis en œuvre une procédure encadrant la restauration des données, et que les opérations de restauration effectuées soient journalisées.	HDS – 4.4.6.3
Outscale met en œuvre une politique de journalisation des événements.	ISO – 12.4.1 SNC – 12.6 a)
Outscale protège l'information journalisée.	ISO – 12.4.2
Outscale s'engage à assurer l'intégrité des journaux.	ISO – 12.4.2 HDS – 4.4.6.10P
Outscale s'engage à protéger les journaux contre les accès illicites.	ISO – 12.4.2 HDS – 4.4.6.10P
Outscale conserve les événements issus de la journalisation.	HDS – 4.4.6.10P
Outscale s'engage à conserver les événements issus de la journalisation pendant une durée minimale de 6 (six) mois.	SNC – 12.6 c)
Outscale s'engage à fournir au client, qui en fait la demande, l'ensemble des événements le concernant dans la limite des durées de conservation légales de ces données applicables à Outscale	HDS – 4.4.6.10C SNC – 12.6 d)
Outscale s'engage à journaliser les activités des administrateurs système et des opérateurs techniques.	ISO – A12.4.3 SNC – 12.6 b)
Outscale s'engage à générer et collecter tout événement lié à la sécurité de l'information.	SNC – 12.6 b)
Outscale transfère les événements journalisés sur des serveurs dédiés distincts de ceux qui les ont générées.	SNC – 12.7 c)
Outscale doit limiter l'accès aux événements journalisés.	SNC – 12.7 d)
Outscale met en œuvre une synchronisation des horloges sur une source de référence temporelle unique.	ISO – A12.4.4 SNC – 12.8 a)
Outscale met en place l'horodatage de chaque événement journalisé.	SNC – 12.8 b)
Outscale s'engage à protéger les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité.	SNC – 12.7 a)

Outscale s'engage à gérer le dimensionnement de l'espace de stockage de l'ensemble des équipements prenant en compte les évolutions du système d'information.	SNC – 12.7 b)
Outscale s'engage à mettre en œuvre une infrastructure permettant l'analyse et la corrélation des événements enregistrés par le système de journalisation pour détecter les événements susceptibles d'affecter la sécurité du SI du Service avec des alarmes quotidiennes d'analyse.	SNC – 12.9 a)
Outscale s'engage à traiter les alarmes remontées par l'infrastructure d'analyse et de corrélation des événements quotidiennement.	SNC – 12.9 c)
Outscale met en œuvre une procédure de contrôle de l'installation de logiciels sur les équipements du SI du Service.	SNC – 12.10 a)
Outscale met en œuvre une procédure de gestion de la configuration des environnements logiciels disponibles pour le client.	SNC – 12.10 b)
Outscale met en œuvre une gestion des vulnérabilités techniques.	SNC – 12.11 a) ISO – A12.6.1
Outscale évalue son exposition à ces vulnérabilités dans son appréciation des risques et applique les mesures de traitement du risque adaptées.	SNC – 12.11 b)
Outscale met en œuvre une procédure obligeant les administrateurs d'Outscale à utiliser des terminaux dédiés à la réalisation exclusive des tâches d'administration.	SNC – 12.12 b)
Outscale met en place des mesures de durcissement pour les terminaux utilisés pour les tâches d'administration.	SNC – 12.12 b)
Outscale met en œuvre une politique pour couvrir les situations de mobilité pour les administrateurs sous sa responsabilité, incluant le chiffrement du disque et l'utilisation d'un tunnel chiffré pour l'ensemble des flux d'administration.	SNC – 12.12 c)
Outscale maintient un plan de capacité prenant en compte les ressources humaines, techniques, financières et d'information, et en assure la surveillance.	HDS – 4.3.3.2
Outscale surveille la capacité en ressources de toutes ses régions cloud.	HDS – 4.3.3.2
Outscale s'assure que les installations ou les mises à jour logicielles sont déployées et qualifiées dans les environnements de test avant d'être mises en production.	HDS – 4.3.2.1
Outscale effectue ses meilleurs efforts afin que les changements opérés sur l'Infrastructure Outscale soient testés et qualifiés pour s'assurer de l'absence d'impact négatif sur le fonctionnement, la performance et la sécurité de l'Infrastructure Outscale.	HDS – 4.3.2.1
Outscale met en œuvre des procédures pour contrôler l'installation de logiciel sur des systèmes en exploitation.	ISO – A12.5
Outscale met en œuvre des règles régissant l'installation de logiciels par les utilisateurs.	ISO – A12.6.2
Outscale met en œuvre des exigences relatives à l'audit des systèmes d'information.	ISO – A12.7.1

- Responsabilité du Client

Description	Référentiel
Le Client définit les mesures organisationnelles et techniques nécessaires à garantir le déploiement et l'administration du Système dans l'état de l'art, qu'il agit pour son propre compte ou celui d'un tiers.	-
Il est de la responsabilité du Client de prendre connaissance de la documentation associée aux Services et des recommandations émises par Outscale afin de garantir une utilisation adéquate, correcte et sécurisée du Service.	-
Il est de la responsabilité du Client d'analyser et gérer les risques sur le Système en :	-

- Assurant la formation des personnes habilitées à exploiter les Services et notamment sur les spécificités du cloud ; - Auditant à intervalle régulier les backups, l'intégrité des données et les accès équipements du Système.	
Il est de la responsabilité du Client d'assurer si nécessaire la capacité de son Système à fonctionner de manière nominale d'un point de vue fonctionnel et sécurité même en cas de dégradation du Service, y compris en mettant en place les bonnes pratiques suivantes : - Automatiser les tâches de déploiement et de mise à jour de l'infrastructure. - Déployer son application de manière redondante en répartissant la charge sur des Machines Virtuelles différentes, voire présentes sur des sites indépendants. - Assurer la sauvegarde de manière incrémentale en utilisant différents types ou fournisseurs de stockage. - Séparer les droits d'accès entre les environnements de développement, d'intégration et de production - Protéger ses environnements et son application avec des systèmes de type Antivirus, WAF, Protection DDoS, etc. - S'assurer que les composants logiciels directs ou indirects font l'objet d'une revue de sécurité et ne sont pas exposés à des failles de sécurité avérées.	-

16. Sécurité des communications

- Responsabilité d'Outscale

Description	Référentiel
Outscale s'engage à mettre en œuvre une politique de gestion et de protection des réseaux.	ISO – A13.1.1
Outscale met en œuvre des mesures de cloisonnement appropriées : (i) entre les clients, (ii) entre les systèmes 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.	-
Outscale a défini les exigences de gestion applicables aux Services de réseau internes ou externalisés.	ISO – A13.1.2
Outscale met en œuvre un cloisonnement des réseaux.	ISO – A13.1.3
Outscale met en œuvre et révise, à minima annuellement, la cartographie du système d'information du Service.	SNC – 13.1 a) b)
Outscale met 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.	SNC – 13.2 c) d) e)
Outscale met en œuvre une surveillance des réseaux dans le cadre de la détection d'incidents de sécurité.	SNC – 13.3 a)
Outscale met en œuvre des politiques et des procédures pour protéger le transfert d'information.	ISO – A13.2.1
Outscale s'engage à ce que les données à caractère personnel soient chiffrées avant d'être transmises sur des réseaux publics.	HDS – 4.4.6.6
Outscale a défini des accords en matière de transfert de l'information dans les activités avec les fournisseurs.	ISO – A13.2.2
Outscale s'engage à protéger l'information transitant par la messagerie électronique.	ISO – A13.2.3
Outscale s'engage à restreindre le recours à des copies papier.	HDS – 4.4.6.2
Outscale a défini les exigences en matière d'engagements de confidentialité ou de non-divulgation pour maintenir la sécurité de l'information transférée au sein de son organisation et vers une entité extérieure.	ISO – A13.2.4
Outscale a inclus dans les contrats de travail des salariés une clause de confidentialité, et en cas de recours à de la sous-traitance, cette exigence s'applique également aux prestataires.	HDS – 4.4.6.1

- Responsabilité du Client

Description	Référentiel
Le Client analyse et gère les risques sur les infrastructures virtualisées installées sur la ou les région(s) 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.	SNC 3.2 b)

17. Sécurité des développements

- Responsabilité d'Outscale

Description	Référentiel
Outscale définit les exigences de sécurité de l'information applicables aux systèmes d'information.	ISO – A14.1.1
Outscale définit et applique des règles de développement des logiciels et des systèmes.	ISO – A14.1.2
Outscale met en œuvre, documente et applique des règles de développement sécurisé des logiciels et des systèmes, et forme les personnels concernés.	HDS – 4.3.2.1 SNC – 14.1 a) b)
Outscale met en œuvre des procédures de contrôle des changements.	ISO – A14.1.2 SNC – 14.2 a)
Outscale met en œuvre une procédure de validation des changements.	SNC – 14.2 a)
Outscale s'engage à conserver un historique des versions logiciels et des systèmes mis en œuvre.	SNC – 14.2 c)
Outscale vérifie et teste les changements apportés aux Infrastructures Outscale.	ISO – A14.2.3
Outscale met en œuvre et documente une procédure de contrôle et de validation des changements avant leur mise en production et conserve un historique des versions logicielles et des systèmes et de les tester avant leur mise en production.	HDS - 4.3.2.1 SNC – 14.3 a)
Outscale n'utilise jamais les données de production de ses clients lors de la réalisation des tests. Outscale s'engage à demander l'autorisation préalable du Client pour utiliser les données du client issues de la production à des fins de test et à garantir l'anonymisation et la confidentialité des données.	SNC – 14.7 b)
Outscale s'assure que les exigences de Services sont identifiées en amont des projets et revues dans les différentes phases du projet.	HDS – 4.3.1
Outscale s'assure que les impacts financiers, organisationnels et techniques potentiels sont pris en compte dans la fourniture de Services nouveaux ou modifiés. Le Client est informé de toute modification du Service et des actions nécessaires à mettre en œuvre le cas échéant.	HDS – 4.3.1
Outscale fera ses meilleurs efforts pour prévenir au plus tôt les clients de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le Client.	SNC - 12.2 d
Outscale s'assure que des mesures de chiffrement et d'authentification fortes sont mises en place pour protéger et sécuriser les informations transmises via des services d'application sur des réseaux publics.	ISO – A14.1.3ISO
Outscale met en œuvre une politique de gestion des mises à jour de progiciels.	ISO – A12.2.4
Outscale a établi des principes d'ingénierie de la sécurité des systèmes dans la mise en œuvre de systèmes d'information.	ISO – A14.2.5
Outscale met en œuvre des environnements de développement sécurisé.	ISO – A14.2.6 SNC – 14.4 a)
Outscale protège les environnements de développement.	SNC – 14.4 b)
Outscale supervise et contrôle les activités de développement externalisé.	ISO – A14.2.7 SNC – 14.5 a)
Outscale s'engage à réaliser des tests de fonctionnalité de la sécurité pendant le développement.	ISO – A14.2.8 SNC – 14.6 a)

Outscale met 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.	SNC – 14.6 a)
Outscale met en œuvre des tests de conformité du système pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.	ISO – A14.2.9

- Responsabilité du Client

Description	Référentiel
Le Client met en œuvre une procédure de gestion des changements apportés sur ses Systèmes en vue de maîtriser les impacts sur la sécurité des données (disponibilité, intégrité, confidentialité, traçabilité).	SNC- 14.2 a)

18. Relations avec les fournisseurs

- Responsabilité d'Outscale

Description	Référentiel
Outscale s'engage à tenir à jour une liste de l'ensemble des fournisseurs participant à la mise en œuvre du Service (hébergeur, développeur, intégrateur, archiveur, sous-traitant, etc.) et préciser leur contribution au Service.	SNC - 15.1 b)
Outscale s'engage à mettre en œuvre une politique de gestion pour les Services fournis par des fournisseurs.	ISO – A15.1.1
Outscale s'engage à mettre en place, et de convenir avec les fournisseurs, les exigences de sécurité de l'information pertinente, en fonction du type de prestations fournies.	ISO – A15.1.2 SNC – 15.2 a)
Outscale s'engage à mettre en œuvre des processus et procédures pour garantir la sécurité de l'information dans le cadre de la chaîne d'approvisionnements des produits et/ou Services avec les fournisseurs.	ISO – A15.1.13
Outscale s'engage à contractualiser avec chacun des fournisseurs participant à la mise en œuvre du Service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces fournisseurs respectent les exigences du référentiel SNC.	SNC – 15.2 b)
Outscale définit et attribue les rôles et responsabilités relatives à la modification ou la fin du contrat avec ses fournisseurs.	SNC – 15.2 c)
Outscale met en œuvre une surveillance et une revue des Services assurés par les fournisseurs.	ISO – A15.2.1 HDS – 4.4.6.12 SNC – 15.3 a)
Outscale met en œuvre une gestion des changements apportés dans les Services des fournisseurs.	ISO – A15.2.2 SNC – 15.3 a)
Outscale s'assure que les changements apportés dans les Services assurés par les fournisseurs n'aboutissent pas à une réduction du niveau de sécurité.	HDS - 4.4.6.12 HDS - 4.4.6.13
Outscale s'engage à lister les sous-traitants ultérieurs auxquels elle recourt dans le cadre du traitement des données à caractère personnel réalisé pour le compte du Client et d'informer au préalable le client en cas de modification de cette liste.	HDS - 4.4.4.1 P
Dans le cas de recours à la sous-traitance dans le traitement des données à caractère personnel, Outscale à encadrer contractuellement avec le sous-traitant ultérieur les	HDS – 4.4.6.12

mesures techniques et organisationnelles prévues pour répondre aux objectifs de sécurité et de protection des données à caractère personnel.	
Outscale met en place une liste des fournisseurs participants à la mise en œuvre du Service, et exiger de ces derniers : - un niveau de sécurité équivalent à la politique de sécurité d'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.	SNC – 15.1 a)
Outscale s'engage à mettre en œuvre un suivi des changements apportés par les fournisseurs, et si les changements sont susceptibles d'affecter le niveau de sécurité du système d'information du Service d'en informer sans délais l'ensemble des clients, et mettre en œuvre les mesures nécessaires permettant de rétablir le niveau de sécurité précédent.	SNC – 15.4 b)
Outscale met en œuvre une procédure afin de réviser au moins annuellement les exigences en matière d'engagement de confidentialité ou de non-divulgation vis-à-vis des fournisseurs.	SNC – 15.5 a)

- Responsabilité du Client

Description	Référentiel
Le Client se doit d'informer Outscale s'il n'accepte pas les changements de fournisseurs qui lui ont été notifiés.	-

19. Gestion des incidents

- Responsabilité d'Outscale

Description	Référentiel
Outscale documente et met en œuvre une politique de gestion des incidents, définissant les responsabilités et les procédures en cas d'incident lié à la sécurité de l'information.	ISO – A16.1.1
Outscale a défini 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 Clients concernés, - informer les employés et fournisseurs participant à la mise en œuvre du Service de la procédure de gestion des incidents, et des modalités de déclaration des incidents.	SNC – 16.1 a) b)
Outscale se doit de signaler dans les meilleurs délais, les événements liés à la sécurité de l'information.	ISO – A16.1.2
Outscale se doit de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou Services.	ISO – A16.1.3
Outscale met en œuvre une procédure exigeant de ses employés et des fournisseurs participant à la mise en œuvre du Service qu'ils lui rendent compte de tout incident de sécurité, avéré ou suspecté ainsi que de toute faille de sécurité.	SNC – 16.2 a)
Outscale met en œuvre une procédure permettant à l'ensemble des clients de signaler tout incident de sécurité, avéré ou suspecté et toute faille de sécurité.	SNC – 16.2 b)
Outscale se doit de communiquer sans délai : - aux clients, les incidents de sécurité et les préconisations associées pour en limiter les impacts, et de donner la possibilité aux clients de choisir d'être notifié en fonction du niveau de gravité des incidents, - aux autorités compétentes, les incidents de sécurité.	SNC – 16.2 c) d)
Outscale se doit de documenter l'appréciation des événements et leur qualification en incident de sécurité.	ISO – A16.1.4 SNC – 16.3 a)
Outscale documente l'appréciation des événements et leur qualification en incident de sécurité, et partage ces informations avec le client à sa demande où s'il est impacté.	SNC – 16.3 a)
Outscale met en œuvre une classification des événements de sécurité incluant les violations de données à caractère personnel.	SNC – 16.3 b)
Outscale met en œuvre des procédures de réponse aux incidents liés à la sécurité de l'information.	ISO – A16.1.5
Outscale se doit de notifier le client de toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.	HDS – 4.4.5.1P
Outscale se doit de notifier à la CNIL, toute violation de données à caractère personnel, si elle représente un risque pour les droits et libertés des personnes concernées.	SNC – 16.1 c)
Outscale s'engage à traiter les incidents de sécurité jusqu'à leur résolution et en informer les clients concernés, et garder les éléments de preuve relatifs aux incidents de sécurité pendant la durée légale de conservation de preuves	SNC – 16.4 a) b)
Outscale met en œuvre un processus d'amélioration continue afin de tirer des enseignements des incidents liés à la sécurité de l'information.	ISO – A16.1.6 SNC – 16.5 a)
Outscale met en œuvre des processus de collecte et de protection de preuves.	ISO – A16.1.7 SNC – 16.6 a)

Outscale s'engage à mettre un canal de communication pour la remontée des failles et vulnérabilités. (https://fr.outscale.com/signalement-des-vulnerabilites/)	-

- Responsabilité du Client

Description	Référentiel
Le Client informe Outscale de tout incident de sécurité, avéré ou suspecté ainsi que de toute faille de sécurité dont il a connaissance dans un délai de 24h en remplissant le formulaire de la page internet de signalement des vulnérabilités : https://fr.outscale.com/signalement-des-vulnerabilites/	SNC 16.2 b)
Le Client doit 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 de Prestataire dans le cas d'alertes ou incidents susceptibles de mettre en cause l'infrastructure ou les Services d'hébergement.	SNC 16.2 b

20. Gestion de la continuité d'activité

- Responsabilité d'Outscale

Description	Référentiel
Outscale a déterminé ses exigences de sécurité de l'information dans la gestion de la continuité de l'activité et dans la gestion de la récupération après sinistre.	ISO – A17.1.1
Outscale met en œuvre et maintient des processus, des procédures et des mesures pour garantir le niveau requis de continuité de la sécurité de l'information.	ISO – 17.1.2 SNC – 17.4
Outscale s'engage à vérifier les mesures de continuité de la sécurité de l'information à intervalles réguliers.	ISO – A17.1.3
Outscale a défini 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.	HDS – 4.3.3.1 SNC – 17.2 a) 17.3 b)
Outscale met à disposition du client des informations documentées sur la sauvegarde de son infrastructure technique et les moyens mis à la disposition du client nécessaires à réaliser ses propres sauvegardes dans le cadre de sa continuité ainsi que leurs fonctionnements.	SNC - 17.5 SNC - 17.6
Outscale s'engage à 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 Client).	-
Outscale s'engage à garantir la disponibilité des moyens de traitement de l'information.	ISO – A17.2.1
Outscale a défini une durée de rétention de ses politiques de sécurité et ses procédures opérationnelles.	HDS – 4.4.5.2P
Outscale met en œuvre un plan de continuité d'activité.	HDS – 4.3.3.1

	SNC – 17.1 a)
Outscale s'engage à réviser annuellement, et à chaque changement majeur pouvant avoir un impact sur le Service, son plan de continuité d'activité.	SNC – 17.1 b)
Pour maintenir l'infrastructure Cloud à jour et garantir la bonne qualité des Services, des maintenances matérielles sur les hyperviseurs sont régulièrement planifiées par Outscale sur les différentes Régions. Deux semaines avant la maintenance, un email est automatiquement envoyé aux ClientS concernés avec la liste de leurs Machines Virtuelles impactées. Si le Client n'a pas stoppé ces Machines Virtuelles au moment des opérations de maintenance, elles seront stoppées de manière forcée, ce qui peut endommager les applications du Client. Outscale peut aussi être amenée à faire des maintenances urgentes, en ce cas elle fait ses meilleurs efforts pour prévenir le Client le plus tôt possible.	-

- Responsabilité du Client

Description	Référentiel
Le Client a la responsabilité de mettre en œuvre 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 clients. Le plan de reprise doit comprendre : - des moyens techniques propres aux clients (locaux, équipements) et des procédures pour redémarrer les systèmes/applications 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.	SNC 17.1 a)
Le client est informé que Outscale ne procède pas à une sauvegarde automatique des Données du client et que le client est seul maître de l'utilisation des moyens mis à sa disposition de sauvegarde de Données ou/et de configuration du Système.	SNC - 17.5 - 17. 6 et 19.1 m)

21. Conformité

- Responsabilité d'Outscale

Description	Référentiel
Outscale se doit d'identifier les exigences légales, réglementaires et contractuelles en vigueur et applicables aux Services fournis.	ISO – A18.1.1 SNC – 18.1 a)
Outscale se doit, selon son rôle dans les traitements de données à caractère personnel, de justifier et documenter les choix des mesures techniques et organisationnelles réalisés en vue de répondre aux exigences de protection des données à caractère personnel.	SNC – 18.1 b)
Outscale s'engage à mettre en œuvre un processus de veille actif des exigences légales, réglementaires et contractuelles en vigueur applicables au Service.	SNC – 18.1 e)
Outscale s'engage à mettre en œuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires.	ISO – A18.1.2

Outscale s'engage à mettre en œuvre des procédures appropriées pour protéger les enregistrements de l'organisation afin de satisfaire aux exigences légales, réglementaires ou contractuelles et soutenir les activités essentielles de l'organisation.	ISO – A18.1.3
Outscale s'engage à mettre en œuvre les procédures appropriées pour garantir la protection de la vie privée et la protection des données à caractère personnelles telles que l'exigent la législation et les réglementations applicables, le cas échéant.	ISO – A18.1.4
Outscale s'engage à mettre à disposition les procédures et moyens pour permettre à ses clients de répondre aux demandes d'exercice des droits des personnes concernées. Les droits couverts sont ceux définis par les articles 15 à 22 du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016.	HDS – 4.4.1
Outscale se doit, selon son rôle dans les traitements de données à caractère personnel, de justifier et documenter les choix des mesures techniques et organisationnelles réalisés en vue de répondre aux exigences de protection des données à caractère personnel.	SNC – 18.1 c)
Outscale s'engage à ne traiter les données à caractère personnel uniquement sur instruction documentée du client et ce, en vertu du contrat.	HDS – 4.4.2P
Outscale s'engage à ne pas utiliser les données de santé qu'il héberge à d'autres fins que l'exécution des Services, et s'interdit toute utilisation à des fins marketing, publicitaires, commerciales ou statistiques.	HDS – 4.4.2C
Outscale s'engage à mettre en place les modalités de notification du client en cas de saisie judiciaire, sauf si cette notification lui est interdite.	HDS – 4.4.2P
Outscale s'engage à tenir à jour un registre des demandes d'informations ainsi que des demandes d'exercice des droits afin de conserver une traçabilité de ces demandes et de leur bonne exécution.	HDS – 4.4.3P
Outscale s'engage à mettre en œuvre des mesures cryptographiques conformément aux accords, lois et réglementations applicables.	ISO – A18.1.5
Outscale s'engage à rendre accessible aux clients qui en font la demande les procédures applicables aux Services fournis.	SNC – 18.1 d)
Outscale s'engage à mettre en œuvre des revues régulières des exigences de sécurité définies dans les politiques, les normes et les réglementations applicables.	ISO – 18.2.2
Outscale s'engage à mettre en œuvre des revues régulières des systèmes d'information pour vérifier leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.	ISO – 18.2.3
Outscale s'engage à mettre en œuvre des revues régulières et indépendantes de la sécurité de l'information.	ISO – 18.2.1
Outscale s'engage à mettre en œuvre un programme d'audit en accord avec la gestion du changement, les politiques et les résultats de l'appréciation des risques.	SNC – 18.2 a)
Outscale s'engage à couvrir dans son programme d'audit : l'audit de la configuration des serveurs et équipements réseau ; le test d'intrusion des accès externes et internes ; l'audit de code.	SNC – 18.2 a) b)
Outscale s'engage à faire réaliser un audit annuel par un prestataire qualifié PASSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information).	SNC – 18.2 b)
Outscale s'engage à communiquer aux clients, qui en font la demande, les rapports d'audit de certification pour le périmètre d'hébergement de données de santé.	HDS – 4.5.3
Outscale s'engage à fournir les rapports d'audit de certification à l'organisme de certification, en cas de transfert ou de demande d'équivalence.	HDS – 4.5.3
Outscale s'assure de l'exécution correcte de l'ensemble des procédures de sécurité et de leur conformité avec les politiques et normes de sécurité.	SNC – 18.5 a)
Outscale met en œuvre et documente une politique de conformité technique.	SNC – 18.5 b)

- Responsabilité du Client

Description	Référentiel
Le Client se doit d'informer Outscale si des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques lui sont confiées (notamment relatives à des organismes d'importance vitale, des données bancaires, des données de santé, des systèmes d'information d'importance vitale (SIIV), etc.)	-
Le Client se doit de mettre en œuvre les procédures adéquates, dans le cadre de l'utilisation des Services, permettant de respecter les exigences légales, réglementaires et contractuelles.	-
Le transfert des Données réalisé par le Client est sous son entière responsabilité.	-
Le Client est informé qu'il est tenu de mettre en œuvre un système d'information de santé respectant la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) élaborée par la Délégation à la stratégie des systèmes d'information de santé (DSSIS) du Ministère des affaires sociales et de la santé et l'agence des systèmes d'information partagés de santé (ASIP Santé) et ses référentiels opposables tels que définis dans les textes légaux et réglementaires.	HDS – 4.5.2
Le Client s'engage à respecter la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) et les référentiels opposables à celle-ci.	HDS – 4.5.2
Le Client doit veiller au respect des lois applicables des Services, dans la stricte mesure des dispositions qui sont effectivement applicables au Client.	-
Le Client doit veiller au respect de toutes les réglementations en vigueur applicables à ses Données (et notamment, les données personnelles, les données de santé, les données bancaires, les obligations applicables aux Organismes d'Importance Vitale (OIV), etc.).	-
S'il propose un site Internet ouvert au public, le Client doit s'assurer de respecter toutes les obligations légales à cet égard.	-