Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de services d'informatique en nuage (SecNumCloud)

référentiel d'exigences

Version 3.2.a du 21 septembre 2021

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
30/07/2014	1.3	*Version publiée pour commentaires.*	ANSSI
20/03/2015	2.0	*Version intermédiaire utilisée pour la procédure expérimentale*	ANSSI
08/12/2016	3.0	*Première version applicable.* Modifications principales : • création d'un référentiel par niveau de qualification ; • clarifications apportées à certaines exigences ; • refonte des chapitres 9, 10, 13 et des annexes ; • intégration plus précise des labels PASSI, PRIS et PDIS.	ANSSI
11/06/2016	3.1	*Version prenant en compte le Règlement général sur la protection des données (RGPD).* Modifications principales : • mise en conformité avec le RGPD ; • retrait de la mention d'un niveau de qualification avancé. • précision concernant l'hébergement externe partagé	ANSSI
21/09/2021	3.2.a	*Clarification des exigences relatives à la protection contre toute réglementation extracommunautaire.* *Modifications principales apportées aux chapitres 1.1.1, 1.3.1, 1.3.2,2, 1.3.3, 3.3.2, 4, 5.3, 7.1, 9.7, 10.5, 12.10, 12.13, 13.3, 18.2, 19.1, 19.2, 19.5, 19.6, Annexe 1, Annexe 2*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg

75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

1. Introduction

1.1. Présentation générale

1.1.1. Contexte

L'informatique en nuage (*cloud computing)* peut être définie comme un modèle de gestion informatique permettant l'accès via un réseau à des ressources informatiques partagées et configurables. Ces ressources sont attribuées à la demande et parfois en libre-service.

La différence entre un hébergement externe partagé classique et un hébergement de type informatique en nuage réside dans le fait que ce dernier se distingue parfois par la mise à disposition de ressources de manière dynamique ou automatique, sans intervention humaine de l'hébergeur.

Le présent référentiel s'applique aussi bien aux contextes d'hébergements externes classiques qu'aux contextes d'hébergements de type informatique en nuage.

Les hébergements partagés tendent aujourd'hui à utiliser des plateformes d'informatique en nuage plutôt que des plateformes d'hébergement classique : c'est pourquoi le présent référentiel utilisera le terme « informatique en nuage » pour désigner tout type d'hébergement externe partagé.

Le présent référentiel couvre les services d'informatique en nuage et vise la qualification de prestataires proposant de tels services.

Les prestataires de services d'informatique en nuage fournissent différents services habituellement classés en quatre types d'activité : infrastructure en tant que service (IaaS), conteneur en tant que service (CaaS), plateforme en tant que service (PaaS) et logiciel en tant que service (SaaS). Ces activités sont détaillées dans le chapitre 2.

L'approche consistant à contractualiser spécifiquement la sécurité dans chaque projet d'hébergement externe a montré ses limites : les offres sont le plus souvent intégrées, de sorte qu'une négociation a posteriori par chaque commanditaire est peu envisageable ; de plus, il peut s'avérer délicat d'inciter chaque commanditaire à procéder à des audits réguliers des services offerts.

Une approche centralisée, définissant un référentiel favorisant l'émergence de services qualifiés, a été retenue : elle permet de traiter la problématique sécurité de manière globale et efficace, les prestataires disposant d'un cadre stable dans lequel s'inscrire pour aller vers la qualification et les usagers pouvant fonder leur confiance sur cette qualification.

Le présent référentiel s'appuie notamment sur la norme internationale [ISO27001] dont il reprend d'ailleurs la structure de l'annexe A. Néanmoins, ce référentiel comporte des exigences additionnelles qui le différencient du standard existant et n'induisent pas l'équivalence entre les deux ensembles de règles.

1.1.2. Objet du document

Ce document constitue le référentiel d'exigences applicables à un prestataire de services d'informatique en nuage (SecNumCloud), ci-après dénommé le « prestataire ».

Il a vocation à permettre la qualification de cette famille de prestataires selon les modalités décrites au chapitre 3.

Il permet au commanditaire 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 commanditaire peut accorder au prestataire.

Il peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Il n'exclut ni l'application de la législation et de la réglementation nationale, ni l'application des règles générales imposées aux prestataires en leur qualité de professionnels et notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

Ce référentiel est conçu sans présomption des technologies qui peuvent être utilisées pour implémenter les services. En particulier, l'expression « informatique en nuage » utilisée au sein de ce référentiel ne sous-entend pas forcément l'utilisation de solutions de virtualisation.

1.1.3. Structure du présent document

Le chapitre 1 correspond à l'introduction du présent référentiel.

Le chapitre 2 décrit les activités visées par le présent référentiel.

Le chapitre 3 présente les modalités de la qualification, qui atteste de la conformité des prestataires de services d'informatique en nuage aux exigences qui leur sont applicables.

Le chapitre 4 présente les niveaux de qualification qui font l'objet de la qualification des prestataires de services d'informatique en nuage.

Les chapitres 5 à 19 présentent les exigences que les prestataires qualifiés doivent respecter.

L'Annexe 1 présente les références des textes législatifs, réglementaires, normatifs et autres mentionnés dans le présent référentiel.

L'Annexe 2 présente des recommandations aux commanditaires de prestations de services d'informatique en nuage.

1.2. Identification du document

Le présent référentiel est dénommé « Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

1.3. Acronymes et définitions

1.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
CaaS	*Container as a service*
CNIL	Commission nationale de l'informatique et des libertés
EBIOS	Expression des besoins et identification des objectifs de sécurité
IaaS	*Infrastructure as a service*
PaaS	*Platform as a service*
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection des incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité
SaaS	*Software as a service*
SDN	*Software Defined Network*

1.3.2. Définitions

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.

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 à qualifier.

***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.

Commanditaire – entité faisant appel à un prestataire de services d'informatique en nuage.

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.

Hébergement externe partagé - modèle permettant un accès aisé et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.

Incident lié à la sécurité de l'information – un ou plusieurs événement(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.

Infrastructure technique – ensemble des composants matériels et logiciels nécessaires à la fourniture d'un service d'informatique en nuage (IaaS, CaaS, PaaS, SaaS, etc.).

Interface d'administration – interface logicielle permettant à une entité disposant des privilèges requis (un administrateur, un compte de service, un développeur « DevOps », etc.) de réaliser des actions d'administration d'un système d'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.

Politique – intentions et orientations d'un organisme telles que formalisées par sa direction.

Prestataire – organisme proposant un service d'informatique en nuage et visant la qualification.

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.

Ressources virtualisées – abstraction des ressources matérielles d'un système (CPU, RAM, etc.) qui sont mises à disposition par l'infrastructure technique.

Risque – effet de l'incertitude sur l'atteinte des objectifs. Il est exprimé en termes de combinaison des conséquences d'un événement 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.

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) – ensemble des actions de diagnostic ayant pour finalité la résolution des problèmes rencontrés par les commanditaires. Aucun accès aux données des commanditaires n'est autorisé dans le cadre de ces tâches. 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.

Vulnérabilité – faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces.

1.3.3. Rôles

Administrateur – utilisateur disposant de droits privilégiés lui permettant de réaliser les tâches d'administration qui lui sont attribuées.

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.

Utilisateur – Toute personne disposant d'un compte 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 commanditaire dans le cas d'un service interne, ou de ses propres commanditaires dans le cas d'un service proposé à l'extérieur.

Le rôle d'administrateur d'infrastructure est toujours sous la responsabilité du prestataire.

Selon le mode de partage des responsabilités entre le prestataire et le commanditaire décrit dans la convention de service, des rôles d'administrateur de sécurité, d'administrateur système, d'administrateur réseau... peuvent se trouver sous la responsabilité du prestataire ou celle du commanditaire.

2. Activités visées par le référentiel

Ce chapitre présente les différentes activités traitées dans le référentiel.

2.1. Fourniture de services SaaS

Ce service concerne la mise à disposition par le prestataire d'applications hébergées sur une plateforme d'informatique en nuage. Le commanditaire n'a pas la maîtrise de la plateforme en nuage sous-jacente. Le prestataire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application.

Exemples : « CRM », outils collaboratifs, messagerie, *Business Intelligence*, « ERP », etc.

2.2. Fourniture de services PaaS

Ce service concerne la mise à disposition par le prestataire de plateformes d'hébergement d'applications. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente, gérée et contrôlée par le prestataire (réseau, serveurs, OS, stockage, etc.). Le commanditaire a cependant la maîtrise des applications déployées sur cette plateforme. Il peut aussi avoir la maîtrise de certains services composant cette plateforme ou de certains éléments de configuration suivant la répartition des rôles définie dans le service.

Exemple : framework de type Apache, Tomcat, PHP et MySQL permettant de développer des applications web.

2.3. Fourniture de services CaaS

Ce service concerne la mise à disposition d'environnements d'exécution permettant le déploiement et l'orchestration de conteneurs. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente (réseau, stockage, serveurs, système d'exploitation), gérée et contrôlée par le prestataire. Le commanditaire a cependant la maîtrise des outils systèmes, bibliothèques, intergiciels, et du code de l'application.

2.4. Fourniture de services IaaS

Ce service concerne la mise à disposition de ressources informatiques abstraites (puissance CPU, mémoire, stockage etc.). Le modèle IaaS permet au commanditaire de disposer de ressources externalisées, potentiellement virtualisées. Ce dernier garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu, par exemple).

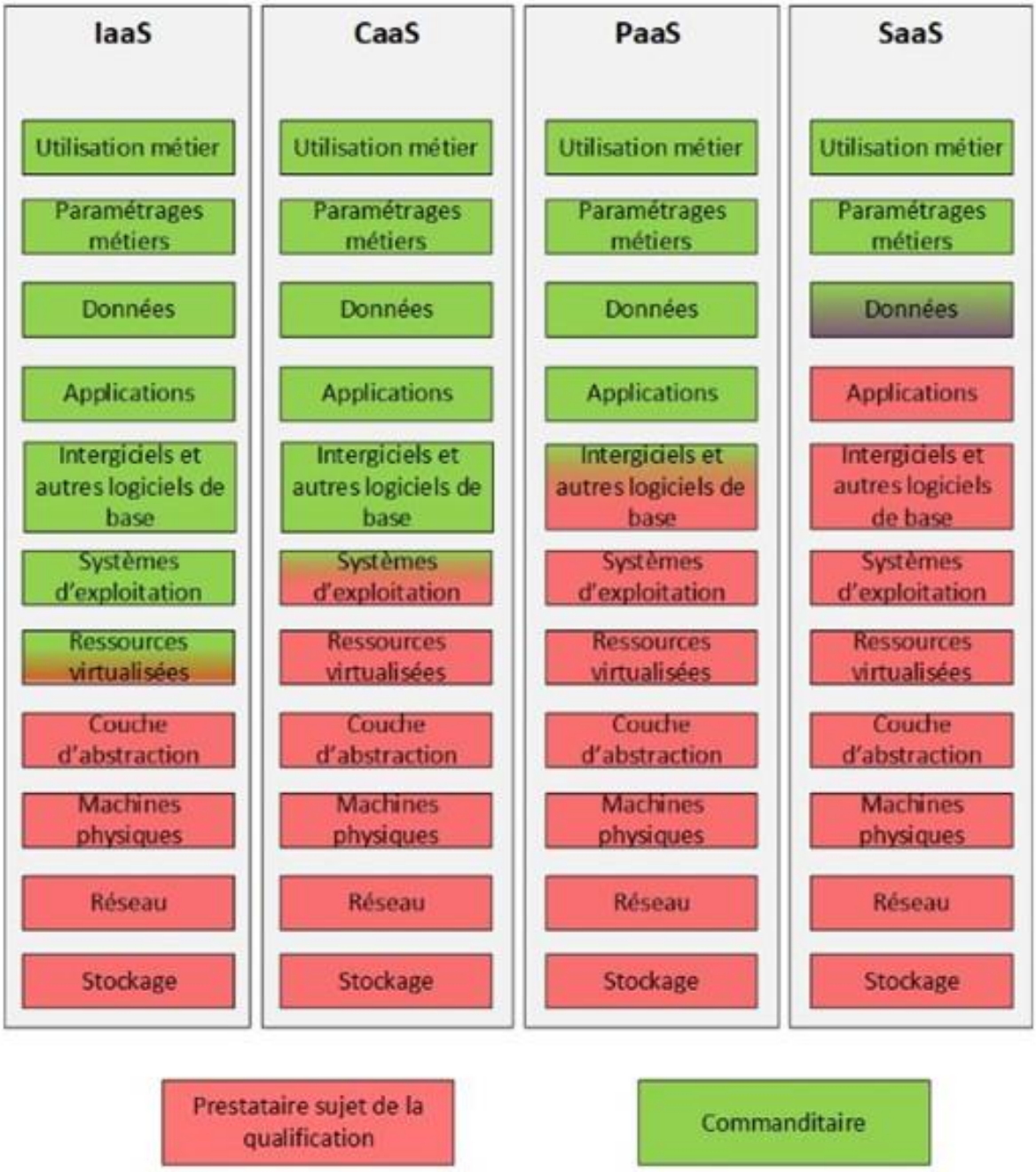

Figure 1 - Répartition des responsabilités par type de service

3. Qualification des prestataires de services d'informatique en nuage

3.1. Modalités de la qualification

Le référentiel contient les exigences et les recommandations à destination des prestataires de services d'informatique en nuage.

La qualification d'un prestataire est réalisée conformément au processus de qualification d'un prestataire de services de confiance [PROCESS_QUALIF] et permet d'attester de la conformité du prestataire aux exigences du référentiel.

Les exigences doivent être respectées par les prestataires pour obtenir la qualification.

Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet de vérification pour obtenir la qualification.

3.2. Portée de la qualification

Pour être qualifié, un prestataire doit répondre à toutes les exigences du présent référentiel sur la portée choisie. La portée est définie par tout ou partie des activités décrites au chapitre 2.

Les prestataires qualifiés gardent la faculté de réaliser des prestations en dehors du périmètre pour lequel ils sont qualifiés, mais ne peuvent, dans ce cas, se prévaloir de la qualification sur ces prestations.

Une prestation de services d'informatique en nuage qualifiée peut être associée à la réalisation d'autres prestations complémentaires (développement, intégration de produits de sécurité, etc.) sans perdre le bénéfice de la qualification.

3.3. Avertissements

3.3.1. Risques liés à l'absence de qualification

Une prestation de services d'informatique en nuage non qualifiée peut potentiellement augmenter l'exposition du commanditaire à certains risques et notamment la fuite d'informations confidentielles, la compromission, la perte ou l'indisponibilité de son système d'information.

Ainsi, dans le cas d'une prestation non qualifiée, il est recommandé au commanditaire d'exiger de la part de son prestataire un document listant l'ensemble des exigences de ce référentiel non couvertes dans le cadre de sa prestation, afin de connaître les risques auxquels il s'expose.

3.3.2. Risques liés à la protection des informations

La conformité au référentiel SecNumCloud ne se substitue pas aux exigences légales ou réglementaires applicables à certaines données spécifiques telles que les données de niveau Diffusion Restreinte ou les données de santé. L'hébergement de données spécifiques dans un service qualifié SecNumCloud nécessite le respect d'exigences complémentaires décrites dans les documents [EX_DONNEES]. L'évaluation du respect de ces exigences complémentaires n'entre pas dans les critères de la qualification SecNumCloud de l'offre du prestataire. Elle doit être prise en compte par le commanditaire dans une démarche d'appréciation des risques de son propre SI avant de recourir aux services du prestataire.

Les clauses de ce référentiel faisant référence à des produits qualifiés sont applicables dans la mesure où ces produits existent.

Par ailleurs, ce référentiel repose sur un objectif de protection des données du commanditaire, mais n'apporte pas de garanties techniques fortes contre un accès du prestataire aux données traitées sur le système d'information du service, uniquement des engagements contractuels. Les commanditaires souhaitant assurer la protection, sur le plan technique, de leurs données contre un accès par le prestataire,

devront par conséquent mettre en œuvre des moyens complémentaires de chiffrement, sous leur maîtrise, de leurs données.

Enfin, il est rappelé que la virtualisation généralement utilisée dans les services d'informatique en nuage ne doit pas être considérée comme un mécanisme de cloisonnement équivalent à une séparation physique.

4. Niveau de sécurité

Le respect des exigences du référentiel SecNumCloud a pour objectif l'atteinte d'un niveau de sécurité permettant le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence limitée pour le commanditaire. Il assure notamment le respect des bonnes pratiques de sécurité relevant de l'hygiène informatique, telles que décrites dans le guide [HYGIENE] de l'ANSSI.

La conformité d'un service d'informatique en nuage à ce référentiel n'atteste pas de sa conformité à la Politique de sécurité des systèmes d'information de l'État [PSSIE].

Le recours, par le commanditaire, à un service qualifié SecNumCloud pour l'hébergement de données soumises à des exigences légales ou réglementaires (telles que les données de niveau Diffusion Restreinte, les données de santé, etc.) nécessite l'évaluation d'exigences complémentaires à mener par le commanditaire dans le cadre d'une démarche d'homologation (cf chapitre 3.3.2) comprenant notamment une appréciation des risques.

5. Politiques de sécurité de l'information et gestion du risque

5.1. Principes

a) Le prestataire doit opérer la prestation à l'état de l'art pour le type d'activité retenu : utiliser des logiciels stables bénéficiant d'un suivi des correctifs de sécurité et paramétrés de façon à obtenir un niveau de sécurité optimal.

b) Le prestataire doit appliquer le guide d'hygiène informatique de l'ANSSI [HYGIENE], niveau renforcé, au système d'information du service.

5.2. Politique de sécurité de l'information

a) Le prestataire doit documenter et mettre en œuvre une politique de sécurité de l'information relative au service.

b) La politique de sécurité de l'information doit identifier les engagements du prestataire quant au respect de la législation et réglementation nationale en vigueur selon la nature des informations qui pourraient être confiées par le commanditaire au prestataire ; il revient en revanche *in fine* au commanditaire de s'assurer du respect des contraintes légales et réglementaires applicables aux données qu'il confie effectivement au prestataire.

c) La politique de sécurité de l'information doit notamment couvrir les thèmes abordés aux chapitres 6 à 19 du présent référentiel.

d) La direction du prestataire doit approuver formellement la politique de sécurité de l'information.

e) Le prestataire doit réviser annuellement la politique de sécurité de l'information et à chaque changement majeur pouvant avoir un impact sur le service.

5.3. Appréciation des risques

a) Le prestataire doit documenter une appréciation des risques couvrant l'ensemble du périmètre du service.

b) Le prestataire doit réaliser son appréciation de risques en utilisant une méthode documentée garantissant la reproductibilité et comparabilité de la démarche.

c) Le prestataire doit prendre en compte dans l'appréciation des risques :

- la gestion d'informations du commanditaire 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 commanditaires ;
- les risques liés à l'effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre commanditaires, 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 ;
- les risques d'atteinte à la confidentialité des données des commanditaires par des tiers impliqués dans la fourniture du service (fournisseurs, sous-traitants, etc.).

d) Le prestataire doit lister, dans un document spécifique, les risques résiduels liés à l'existence de lois extraterritoriales ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable.

e) Le prestataire doit mettre à la disposition du commanditaire, sur demande de celui-ci, les éléments d'appréciation des risques liés à la soumission des données du commanditaire au droit d'un état non-membre de l'Union Européenne.

f) Lorsqu'il existe des exigences légales, réglementaires ou sectorielles spécifiques liées aux types d'informations confiées par le commanditaire au prestataire, ce dernier doit les prendre en compte dans son appréciation des risques en s'assurant de respecter l'ensemble des exigences du présent référentiel d'une part et de ne pas abaisser le niveau de sécurité établi par le respect des exigences du présent référentiel d'autre part.

g) La direction du prestataire doit accepter formellement les risques résiduels identifiés dans l'appréciation des risques.

h) Le prestataire doit réviser annuellement l'appréciation des risques et à chaque changement majeur pouvant avoir un impact sur le service.

6. Organisation de la sécurité de l'information

6.1. Fonctions et responsabilités liées à la sécurité de l'information

a) Le prestataire doit documenter et mettre en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.

b) Le prestataire doit désigner un responsable de la sécurité des systèmes d'information et un responsable de la sécurité physique.

c) Le prestataire doit définir et attribuer les responsabilités en matière de sécurité de l'information pour le personnel impliqué dans la fourniture du service.

d) Le prestataire doit s'assurer après tout changement majeur pouvant avoir un impact sur le service que l'attribution des responsabilités en matière de sécurité de l'information est toujours pertinente.

e) Le prestataire doit définir et attribuer les responsabilités en matière de protection de données à caractère personnel, en cohérence avec son rôle dans les traitements de données à caractère personnel (responsable de traitement, sous-traitant ou co-responsable).

f) Le prestataire doit, lorsqu'il traite un grand nombre de données parmi lesquelles figurent des catégories particulières de données à caractère personnel telles que définies dans [RGPD], désigner un délégué à la protection des données.

g) Il est recommandé que le prestataire, quel que soit le volume de données à caractère personnel qu'il traite, désigne un délégué à la protection des données.

h) Le prestataire doit 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 élevé pour les droits et libertés des personnes concernées (traitement de catégories particulières de données à caractère personnel telles que définies dans [RGPD], traitement de données à grande échelle, etc.). Cette analyse doit comporter une évaluation juridique du respect des principes et droits fondamentaux, ainsi qu'une étude plus technique des mesures techniques mises en œuvre pour protéger les personnes des risques pour leur vie privée.

6.2. Séparation des tâches

a) Le prestataire doit identifier les risques associés à des cumuls de responsabilités ou de tâches, les prendre en compte dans l'appréciation des risques et mettre en œuvre des mesures de réduction de ces risques.

6.3. Relations avec les autorités

a) Il est recommandé que le prestataire mette en place des relations appropriées avec les autorités compétentes en matière de sécurité de l'information et de données à caractère personnel et, le cas échéant, avec les autorités sectorielles selon la nature des informations confiées par le commanditaire au prestataire.

6.4. Relations avec les groupes de travail spécialisés

a) Il est recommandé que le prestataire entretienne des contacts appropriés avec des groupes de spécialistes ou des sources reconnues, notamment pour prendre en compte de nouvelles menaces et les mesures de sécurité appropriées pour les contrer.

6.5. La sécurité de l'information dans la gestion de projet

a) Le prestataire doit documenter une estimation des risques préalablement à tout projet pouvant avoir un impact sur le service, et ce quelle que soit la nature du projet.

b) Dans la mesure où un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, le prestataire doit avertir le commanditaire et l'informer par écrit des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant.

7. Sécurité des ressources humaines

7.1. Sélection des candidats

a) Le prestataire doit documenter et mettre en œuvre une procédure de vérification des informations concernant son personnel conforme aux lois et règlements en vigueur.

Ces vérifications s'appliquent à toute personne impliquée dans la fourniture du service et doivent être proportionnelles à la sensibilité ou à la spécificité des informations du commanditaire confiées au prestataire ainsi qu'aux risques identifiés.

b) Le prestataire doit renforcer ces vérifications lorsqu'il s'agit de personnels disposant de privilèges d'administration élevés sur les composants logiciels et matériels de l'infrastructure du service. Il est entendu par des privilèges d'administration élevés, des actions permettant l'élévation de privilèges ou la possibilité de réaliser des actions sans traces techniques ou de désactiver, altérer les traces techniques.

7.2. Conditions d'embauche

a) Le prestataire doit disposer d'une charte d'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 ne recourent qu'aux méthodes, outils et techniques validés par le prestataire ;
- les personnels s'engagent à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation sauf autorisation formelle et écrite du commanditaire ;
- les personnels s'engagent à signaler au prestataire tout contenu manifestement illicite découvert pendant la prestation ;
- les personnels s'engagent à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités.

b) Le prestataire doit faire signer la charte d'éthique à l'ensemble des personnes impliquée dans la fourniture du service.

c) Le prestataire doit introduire, dans le contrat de travail des personnels disposant de privilèges d'administration élevés sur les composants et matériels de l'infrastructure du service, un engagement de responsabilité avec un renvoi aux clauses du code du travail sur la protection du secret des affaires et de la propriété intellectuelle. Il est entendu par des privilèges d'administration élevés, des actions permettant l'élévation de privilèges ou la possibilité de réaliser des actions sans traces techniques ou de désactiver, altérer les traces techniques.

d) Le prestataire doit, sur demande d'un commanditaire, lui rendre accessible le règlement intérieur et la charte d'éthique.

7.3. Sensibilisation, apprentissage et formations à la sécurité de l'information

a) Le prestataire doit sensibiliser à la sécurité de l'information et aux risques liés à la protection des données l'ensemble des personnes impliquées dans la fourniture du service. Il doit leur communiquer les mises à jour des politiques et procédures pertinentes dans le cadre de leurs missions.

b) Le prestataire doit documenter et mettre en œuvre un plan de formation concernant la sécurité de l'information adapté au service et aux missions des personnels.

c) Le responsable de la sécurité des systèmes d'information du prestataire doit valider formellement le plan de formation concernant la sécurité de l'information.

7.4. Processus disciplinaire

a) Le prestataire doit documenter et mettre en œuvre un processus disciplinaire applicable à l'ensemble des personnes impliquées dans la fourniture du service ayant enfreint la politique de sécurité.

b) Le prestataire doit, sur demande d'un commanditaire, lui rendre accessible les sanctions encourues en cas d'infraction à la politique de sécurité.

7.5. Rupture, terme ou modification du contrat de travail

a) Le prestataire doit définir et attribuer les rôles et les responsabilités relatives 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

8.1. Inventaire et propriété des actifs

a) Le prestataire doit tenir à jour l'inventaire de l'ensemble des équipements mettant en œuvre le service. Cet inventaire doit préciser pour chaque équipement :

- les informations d'identification de l'équipement (nom, adresse IP, adresse MAC, etc.) ;
- la fonction de l'équipement ;
- le modèle de l'équipement ;
- la localisation de l'équipement ;
- le propriétaire de l'équipement ;
- le besoin de sécurité des informations (au sens du chapitre 8.3).

b) Le prestataire doit tenir à jour l'inventaire de l'ensemble des logiciels mettant en œuvre le service. Cet inventaire doit identifier pour chaque logiciel, sa version et les équipements sur lesquels le logiciel est installé.

c) Le prestataire doit s'assurer de la validité des licences des logiciels tout au long de la prestation.

8.2. Restitution des actifs

a) Le prestataire doit documenter et 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.

8.3. Identification des besoins de sécurité de l'information

a) Le prestataire doit identifier les différents besoins de sécurité des informations relatives au service.

b) Lorsque le commanditaire confie au prestataire des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques, le prestataire doit identifier les besoins de sécurité spécifiques associés à ces contraintes.

8.4. Marquage et manipulation de l'information

a) Il est recommandé que le prestataire documente et mette en œuvre une procédure pour le marquage et la manipulation de toutes les informations participant à la délivrance du service, conformément à son besoin de sécurité défini au chapitre 8.3.

8.5. Gestion des supports amovibles

a) Le prestataire doit documenter et mettre en œuvre une procédure pour la gestion des supports amovibles, conformément au besoin de sécurité défini au chapitre 8.3.

Lorsque des supports amovibles sont utilisés sur l'infrastructure technique ou pour des tâches d'administration, ces supports doivent être dédiés à un usage.

9. Contrôle d'accès et gestion des identités

Sauf mention explicite, ce chapitre concerne le contrôle d'accès et la gestion des identités des utilisateurs :

- placés sous la responsabilité du prestataire (ses employés et éventuellement des tiers participant à la fourniture du service) ;
- placés sous la responsabilité du commanditaire, mais pour lesquels le prestataire met en œuvre les moyens de contrôle d'accès (en fournissant notamment au commanditaire une interface de gestion des comptes et des droits d'accès).

Les utilisateurs pour lesquels le commanditaire met en œuvre les moyens de contrôle d'accès et de gestion des identités sont hors du champ d'application de ce référentiel.

9.1. Politiques et contrôle d'accès

a) Le prestataire doit documenter et mettre en œuvre une politique de contrôle d'accès sur la base du résultat de son appréciation des risques et du partage des responsabilités.

b) Le prestataire doit réviser annuellement la politique de contrôle d'accès et à chaque changement majeur pouvant avoir un impact sur le service.

9.2. Enregistrement et désinscription des utilisateurs

a) Le prestataire doit documenter et mettre en œuvre une procédure d'enregistrement et de désinscription des utilisateurs s'appuyant sur une interface de gestion des comptes et des droits d'accès. Cette procédure doit indiquer quelles données doivent être supprimées au départ d'un utilisateur.

b) Le prestataire doit attribuer des comptes nominatifs lors de l'enregistrement des utilisateurs placés sous sa responsabilité.

c) Le prestataire doit mettre en œuvre des moyens permettant de s'assurer que la désinscription d'un utilisateur entraîne la suppression de tous ses accès aux ressources du système d'information du service, ainsi que la suppression de ses données conformément à la procédure d'enregistrement et de désinscription (voir exigence 9.2 a)).

9.3. Gestion des droits d'accès

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'assurer l'attribution, la modification et le retrait de droits d'accès aux ressources du système d'information du service.

b) Le prestataire doit mettre à la disposition de ses commanditaires les outils et les moyens qui permettent une différenciation des rôles des utilisateurs du service, par exemple suivant leur rôle fonctionnel.

c) Le prestataire doit tenir à jour l'inventaire des utilisateurs sous sa responsabilité disposant de droits d'administration sur les ressources du système d'information du service.

d) Le prestataire doit être en mesure de fournir, pour une ressource donnée mettant en œuvre le service, la liste de tous les utilisateurs y ayant accès, qu'ils soient sous la responsabilité du prestataire ou du commanditaire ainsi que les droits d'accès qui leurs ont été attribués.

e) Le prestataire doit être en mesure de fournir, pour un utilisateur donné, qu'ils soient sous la responsabilité du prestataire ou du commanditaire, la liste de tous ses droits d'accès sur les différents éléments du système d'information du service.

f) Le prestataire doit définir une liste de droits d'accès incompatibles entre eux. Il doit s'assurer, lors de l'attribution de droits d'accès à un utilisateur qu'il ne possède pas de droits d'accès incompatibles entre eux au titre de la liste précédemment établie.

g) Le prestataire doit inclure dans la procédure de gestion des droits d'accès les actions de révocation ou de suspension des droits de tout utilisateur.

9.4. Revue des droits d'accès utilisateurs

a) Le prestataire doit réviser annuellement les droits d'accès des utilisateurs sur son périmètre de responsabilité.

b) Le prestataire doit mettre à disposition du commanditaire un outil facilitant la revue des droits d'accès des utilisateurs placés sous la responsabilité de ce dernier.

c) Le prestataire doit réviser trimestriellement la liste des utilisateurs sur son périmètre de responsabilité pouvant utiliser les comptes techniques mentionnés dans l'exigence 9.2 b).

9.5. Gestion des authentifications des utilisateurs

a) Le prestataire doit formaliser et mettre en œuvre des procédures de gestion de l'authentification des utilisateurs. En accord avec les exigences du chapitre 10, celles-ci doivent notamment porter sur :

- la gestion des moyens d'authentification (émission et réinitialisation de mot de passe, mise à jour des CRL et import des certificats racines en cas d'utilisation de certificats, etc.).
- la mise en place des moyens permettant une authentification à multiples facteurs afin de répondre aux différents cas d'usage du référentiel.
- les systèmes qui génèrent des mots de passe ou vérifient leur robustesse, lorsqu'une authentification par mot de passe est utilisée. Ils doivent suivre les recommandations de [NT_MDP].

b) Tout mécanisme d'authentification doit prévoir le blocage d'un compte après un nombre limité de tentatives infructueuses.

c) Dans le cadre d'un service SaaS, le prestataire doit proposer à ses commanditaires des moyens d'authentification à multiples facteurs pour l'accès des utilisateurs finaux.

d) Lorsque des comptes techniques, non nominatifs, sont nécessaires, le prestataire doit mettre en place des mesures obligeant les utilisateurs à s'authentifier avec leur compte nominatif avant de pouvoir accéder à ces comptes techniques.

9.6. Accès aux interfaces d'administration

a) Les comptes d'administration sous la responsabilité du prestataire doivent être gérés à l'aide d'outils et d'annuaires distincts de ceux utilisés pour la gestion des comptes utilisateurs placés sous la responsabilité du commanditaire.

b) Les interfaces d'administration mises à disposition des commanditaires doivent être distinctes des interfaces d'administration utilisées par le prestataire.

c) Les interfaces d'administration mises à disposition des commanditaires ne doivent permettre aucune connexion avec des comptes d'administrateurs sous la responsabilité du prestataire.

d) Les interfaces d'administration utilisées par le prestataire ne doivent pas être accessibles à partir d'un réseau public et ainsi ne doivent permettre aucune connexion des utilisateurs sous la responsabilité du commanditaire.

e) Si des interfaces d'administration sont mises à disposition des commanditaires avec un accès via un réseau public, les flux d'administration doivent être authentifiés et chiffrés avec des moyens en accord avec les exigences du chapitre 10.2.

f) Le prestataire doit mettre en place un système d'authentification à double facteur pour l'accès :

- aux interfaces d'administration utilisées par le prestataire ;
- aux interfaces d'administration dédiées aux commanditaires.

g) Dans le cadre d'un service SaaS, les interfaces d'administration mises à disposition des commanditaires doivent être différenciées des interfaces permettant l'accès des utilisateurs finaux.

h) Dès lors qu'une interface d'administration est accessible depuis un réseau public, le processus d'authentification doit avoir lieu avant toute interaction entre l'utilisateur et l'interface en question.

i) Lorsque le prestataire utilise un service de type IaaS comme socle d'un autre type de service (CaaS, PaaS ou SaaS), les ressources affectées à l'usage du prestataire ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres commanditaires du service IaaS.

j) Lorsque le prestataire utilise un service de type CaaS comme socle d'un autre type de service (PaaS ou SaaS), les ressources affectées à l'usage du prestataire ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres commanditaires du service CaaS.

k) Lorsque le prestataire utilise un service de type PaaS comme socle d'un autre type de service (typiquement SaaS), les ressources affectées à l'usage du prestataire ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres commanditaires du service PaaS.

9.7. Restriction des accès à l'information

a) Le prestataire doit mettre en œuvre des mesures de cloisonnement appropriées entre ses commanditaires.

b) Le prestataire doit mettre en œuvre des mesures de cloisonnement appropriées entre le système d'information du service et ses autres systèmes d'information (bureautique, informatique de gestion, gestion technique du bâtiment, contrôle d'accès physique, etc.).

c) Le prestataire doit concevoir, développer, configurer et déployer le système d'information du service en assurant au moins un cloisonnement entre d'une part l'infrastructure technique et d'autre part les équipements nécessaires à l'administration des services et des ressources qu'elle héberge.

d) Dans le cadre du support technique, si les actions nécessaires au diagnostic et à la résolution d'un problème rencontré par un commanditaire nécessitent un accès aux données du commanditaire, alors le prestataire doit :

- n'autoriser l'accès aux données du commanditaire qu'après consentement explicite du commanditaire ;
- vérifier que la personne à qui l'accès doit être autorisé a satisfait aux vérifications de l'exigence 7.1.a) relative à la sensibilité ou à la spécificité des données du commanditaire ;
- vérifier que la personne à qui l'accès doit être autorisé est localisée au sein de l'Union Européenne ;
- dans le cas d'une intervention réalisée à distance par une personne n'ayant pas satisfait aux vérifications de l'exigence 7.1.a), mettre en œuvre une passerelle sécurisée (poste de rebond) par laquelle la personne devra se connecter et permettant une supervision (autorisation ou interdiction des actions, demander d'explications, etc..) en temps réel, par une personne ayant elle-même satisfait aux vérifications de l'exigence 7.1.a) ;
- considérer les actions menées, une fois l'accès autorisé, comme des actions d'administration et les journaliser comme telles ;

- supprimer l’autorisation d’accès aux données du commanditaire au terme de ces actions.

10. Cryptologie

10.1. Chiffrement des données stockées

a) Le prestataire doit définir et mettre en œuvre un mécanisme de chiffrement empêchant la récupération des données des commanditaires en cas de réallocation d'une ressource ou de récupération du support physique.

- dans le cas d'un service IaaS ou CaaS, cet objectif pourra par exemple être atteint :
    - par un chiffrement du disque ou du système de fichier, lorsque le protocole d'accès en mode fichiers garantit que seuls des blocs vides peuvent être alloués (par exemple stockage de type NAS dans lequel un bloc physique n'est effectivement affecté qu'au moment de l'écriture),
    - par un chiffrement par volume dans le cas d'un accès en mode bloc (par exemple stockage de type SAN ou stockage local), avec au moins une clé par commanditaire ;
- dans le cas d'un service PaaS ou SaaS, cet objectif pourra être atteint en utilisant un chiffrement applicatif dans le périmètre du prestataire, avec au moins une clé par commanditaire.

b) Le prestataire doit utiliser une méthode de chiffrement des données respectant les règles de [CRYPTO_B1].

c) Il est recommandé d'utiliser une méthode de chiffrement des données respectant les recommandations de [CRYPTO_B1].

d) Le prestataire doit mettre en place un chiffrement des données sur les supports amovibles et les supports de sauvegarde amenés à quitter le périmètre de sécurité physique du système d'information du service (au sens du chapitre 10), en fonction du besoin de sécurité des données (voir chapitre 8.3).

10.2. Chiffrement des flux

a) Lorsque le prestataire met en œuvre un mécanisme de chiffrement des flux réseau, celui-ci doit respecter les règles de [CRYPTO_B1].

b) Lorsque le prestataire met en œuvre un mécanisme de chiffrement des flux réseau, il est recommandé que celui-ci respecte les recommandations de [CRYPTO_B1].

c) Si le protocole TLS est mis en œuvre, le prestataire doit appliquer les recommandations de [NT_TLS].

d) Si le protocole IPsec est mis en œuvre, le prestataire doit appliquer les recommandations de [NT_IPSEC].

e) Si le protocole SSH est mis en œuvre, le prestataire doit appliquer les recommandations de [NT_IPSEC].

10.3. Hachage des mots de passe

a) Le prestataire ne doit stocker que l'empreinte des mots de passe des utilisateurs et des comptes techniques.

b) Le prestataire doit mettre en œuvre une fonction de hachage respectant les règles de [CRYPTO_B1]

c) Il est recommandé que le prestataire mette en œuvre une fonction de hachage respectant les recommandations de [CRYPTO_B1].

d) Le prestataire doit générer les empreintes des mots de passe avec une fonction de hachage associée à l'utilisation d'un sel cryptographique respectant les règles de [CRYPTO_B1].

10.4. Non répudiation

a) Lorsque le prestataire met en œuvre un mécanisme de signature électronique, celui-ci doit respecter les règles de [CRYPTO_B1]

b) Lorsque le prestataire met en œuvre un mécanisme de signature électronique, il est recommandé que celui-ci respecte les recommandations de [CRYPTO_B1].

10.5. Gestion des secrets

a) Le prestataire doit mettre en œuvre des clés cryptographiques respectant les règles de [CRYPTO_B2].

b) Il est recommandé que le prestataire mette en œuvre des clés cryptographiques respectant les recommandations de [CRYPTO_B2].

c) Le prestataire doit protéger l'accès aux clés cryptographiques et autres secrets utilisés pour le chiffrement des données par un moyen adapté : conteneur de sécurité (logiciel ou matériel) ou support disjoint.

d) Le prestataire doit protéger l'accès aux clés cryptographiques et autres secrets utilisés pour les tâches d'administration par un conteneur de sécurité adapté, logiciel ou matériel.

10.6. Racines de confiance

a) Sur l'infrastructure technique, le prestataire doit utiliser exclusivement des certificats de clé publique issus d'une autorité de certification d'un état membre de l'Union Européenne (les cérémonies de génération des clés maîtresses doivent avoir lieu dans un pays membre de l'Union Européenne et en présence du prestataire).

11. Sécurité physique et environnementale

11.1. Périmètres de sécurité physique

a) Le prestataire doit documenter et mettre en œuvre des périmètres de sécurité, incluant le marquage des zones et les différents moyens de limitation et de contrôle des accès.

b) Le prestataire doit distinguer des zones publiques, des zones privées et des zones sensibles.

11.1.1. Zones publiques

a) Les zones publiques sont accessibles à tous dans les limites de la propriété du prestataire. Le prestataire ne doit héberger aucune ressource dévolue au service ou permettant d'accéder à des composantes de celui-ci dans les zones publiques.

11.1.2. Zones privées

a) Les zones privées peuvent héberger :

- les plateformes et moyens de développement du service ;
- les postes d'administration, d'exploitation et de supervision ;
- les locaux à partir desquels le prestataire opère.

11.1.3. Zones sensibles

a) Les zones sensibles sont réservées à l'hébergement du système d'information de production du service hors postes d'administration, d'exploitation et de supervision.

11.2. Contrôle d'accès physique

11.2.1. Zones privées

a) Le prestataire doit protéger les zones privées contre les accès non autorisés. Pour ce faire, il doit mettre en œuvre un contrôle d'accès physique reposant au moins sur un facteur personnel : la connaissance d'un secret, la détention d'un objet ou la biométrie.

b) Il est recommandé que le prestataire respecte les recommandations de [G_SANSCONTACT] pour mettre en œuvre du contrôle d'accès physique.

c) Le prestataire doit définir et documenter des mesures d'accès physique dérogatoires en cas d'urgence.

d) Le prestataire doit afficher à l'entrée des zones privées un avertissement relatif aux limites et conditions d'accès à ces zones.

e) Le prestataire doit définir et documenter les plages horaires et conditions d'accès aux zones privées en fonction des profils des intervenants.

f) Le prestataire doit documenter et mettre en œuvre les moyens permettant de s'assurer que les visiteurs sont systématiquement accompagnés par le prestataire lors de leurs accès et séjours en zone privée. Le prestataire doit conserver une trace de l'identité des visiteurs conformément à la législation et réglementation en vigueur.

g) En cas d'intervention (actions de diagnostic, de maintenance, ou d'administration) en zone privée par un tiers visiteur, le prestataire doit faire superviser (suivre, autoriser, interdire, questionner) les actions par un personnel ayant satisfait aux vérifications de l'exigence 7.1.a) .

h) Le prestataire doit documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones privées.

11.2.2. Zones sensibles

a) Le prestataire doit protéger les zones sensibles contre les accès non autorisés. Pour ce faire, il doit mettre en œuvre un contrôle d'accès physique reposant au moins sur deux facteurs personnels : la connaissance d'un secret, la détention d'un objet ou la biométrie.

b) Il est recommandé que le prestataire respecte les recommandations de [G_SANSCONTACT] pour la mise en œuvre du contrôle d'accès physique.

c) Le prestataire doit définir et documenter des mesures d'accès physique dérogatoires en cas d'urgence.

d) Le prestataire doit afficher à l'entrée des zones sensibles un avertissement relatif aux limites et conditions d'accès à ces zones.

e) Le prestataire doit définir et documenter les plages horaires et conditions d'accès aux zones sensibles en fonction des profils des intervenants.

f) Le prestataire doit documenter et mettre en œuvre les moyens permettant de s'assurer que les visiteurs sont systématiquement accompagnés par le prestataire lors de leurs accès et séjours en zone sensible. Le prestataire doit conserver une trace de l'identité des visiteurs conformément à la législation et réglementation en vigueur.

g) En cas d'intervention (actions de diagnostic, de maintenance, ou d'administration) en zone sensible par un tiers visiteur, le prestataire doit faire superviser (suivre, autoriser, interdire, questionner) les actions par un personnel ayant satisfait aux vérifications de l'exigence 7.1.a. .

h) Le prestataire doit documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones sensibles.

i) Le prestataire doit mettre en place une journalisation des accès physiques aux zones sensibles. Il doit effectuer une revue de ces journaux au moins mensuellement.

j) Le prestataire doit mettre en œuvre les moyens garantissant qu'aucun accès direct n'existe entre une zone publique et une zone sensible.

11.3. Protection contre les menaces extérieures et environnementales

a) Le prestataire doit documenter et mettre en œuvre les moyens permettant de minimiser les risques inhérents aux sinistres physiques (incendie, dégât des eaux, etc.) et naturels (risques climatiques, inondations, séismes, etc.).

b) Le prestataire doit documenter et mettre en œuvre les mesures permettant de limiter les risques de départ et de propagation de feu ainsi que les risques de dégât des eaux.

c) Le prestataire doit documenter et mettre en œuvre les mesures permettant de prévenir et limiter les conséquences d'une coupure d'alimentation électrique et permettre une reprise du service conformément aux exigences de disponibilité du service définies dans la convention de service.

d) Le prestataire doit documenter et mettre en œuvre les moyens permettant de maintenir des conditions de température et d'humidité adaptées aux équipements. De plus, il doit mettre en œuvre des mesures permettant de prévenir les pannes de climatisation et d'en limiter les conséquences.

e) Le prestataire doit documenter et mettre en œuvre des contrôles et tests réguliers des équipements de détection et de protection physique.

11.4. Travail dans les zones privées et sensibles

a) Le prestataire doit intégrer les éléments de sécurité physique dans la politique de sécurité et l'appréciation des risques conformément au niveau de sécurité requis par la catégorie de la zone.

b) Le prestataire doit documenter et mettre en œuvre des procédures relatives au travail en zones privées et sensibles. Il doit communiquer ces procédures aux intervenants concernés.

11.5. Zones de livraison et de chargement

b) Les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux sans être accompagnées sont considérées comme des zones publiques.

c) Le prestataire doit isoler les points d'accès de ces zones vers les zones privées et sensibles, de façon à éviter les accès non autorisés, ou à défaut, implémenter des mesures compensatoires permettant d'assurer le même niveau de sécurité.

11.6. Sécurité du câblage

a) Le prestataire doit documenter et mettre en œuvre des mesures permettant de protéger le câblage électrique et de télécommunication des dommages physiques et des possibilités d'interception.

b) Le prestataire doit établir et tenir à jour un plan de câblage.

c) Il est recommandé que le prestataire mette en œuvre des mesures permettant d'identifier les câbles (par exemple code couleur, étiquette, etc.) afin d'en faciliter l'exploitation et limiter les erreurs de manipulation.

11.7. Maintenance des matériels

a) Le prestataire doit documenter 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 hébergés en zones privés et sensibles sont compatibles avec les exigences de confidentialité et de disponibilité du service définies dans la convention de service.

b) Le prestataire doit souscrire des contrats de maintenance permettant de disposer des mises à jour de sécurité des logiciels installés sur les équipements du système d'information du service.

c) Le prestataire doit s'assurer que les supports ne peuvent être retournés à un tiers que si les données du commanditaire y sont stockées chiffrées conformément au chapitre 10.1 ou ont préalablement été détruites à l'aide d'un mécanisme d'effacement sécurisé par réécriture de motifs aléatoires.

d) Le prestataire doit documenter et mettre en œuvre des mesures permettant de s'assurer que les conditions d'installation, de maintenance et d'entretien des équipements techniques annexes (alimentation électrique, climatisation, incendie, etc.) sont compatibles avec les exigences de disponibilité du service définies dans la convention de service.

11.8. Sortie des actifs

a) Le prestataire doit documenter et mettre en œuvre une procédure de transfert hors site de données du commanditaire, équipements et logiciels. Cette procédure doit nécessiter que la direction du prestataire donne son autorisation écrite. Dans tous les cas, le prestataire doit mettre en œuvre les moyens permettant de garantir que le niveau de protection en confidentialité et en intégrité des actifs durant leur transport est équivalent à celui sur site.

11.9. Recyclage sécurisé du matériel

a) Le prestataire doit documenter et mettre en œuvre des moyens permettant d'effacer de manière sécurisée par réécriture de motifs aléatoires tout support de données mis à disposition d'un commanditaire. Si l'espace de stockage est chiffré dans le cadre de l'exigence 10.1.a), l'effacement peut être réalisé par un effacement sécurisé de la clé de chiffrement.

11.10. Matériel en attente d'utilisation

a) Le prestataire doit documenter et mettre en œuvre une procédure de protection du matériel en attente d'utilisation.

12. Sécurité liée à l'exploitation

12.1. Procédures d'exploitation documentées

a) Le prestataire doit documenter les procédures d'exploitation, les tenir à jour et les rendre accessibles au personnel concerné.

12.2. Gestion des changements

a) Le prestataire doit documenter et mettre en œuvre une procédure de gestion des changements apportés aux systèmes et moyens de traitement de l'information.

b) Le prestataire doit documenter et mettre en œuvre une procédure permettant, en cas d'opérations réalisées par le prestataire et pouvant avoir un impact sur la sécurité ou la disponibilité du service, de communiquer au plus tôt à l'ensemble de ses commanditaires les informations suivantes :

- la date et l'heure programmées du début et de la fin des opérations;
- la nature des opérations ;
- les impacts sur la sécurité ou la disponibilité du service ;
- le contact au sein du prestataire.

c) Dans le cadre d'un service PaaS, le prestataire doit informer au plus tôt le commanditaire de toute modification à venir sur des éléments logiciels sous sa responsabilité dès lors que la compatibilité complète ne peut être assurée.

d) Le prestataire doit informer au plus tôt le commanditaire de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le commanditaire.

12.3. Séparation des environnements de développement, de test et d'exploitation

a) Le prestataire doit documenter et mettre en œuvre les mesures permettant de séparer physiquement les environnements liés à la production du service des autres environnements, dont les environnements de développement.

12.4. Mesures contre les codes malveillants

a) Le prestataire doit documenter et mettre en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants. Le périmètre d'application de cette exigence sur le système d'information du service doit nécessairement contenir les postes utilisateurs sous la responsabilité du prestataire et les flux entrants sur ce même système d'information.

b) Le prestataire doit documenter et mettre en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.

12.5. Sauvegarde des informations

a) Le prestataire doit documenter et mettre en œuvre une politique de sauvegarde et de restauration des données sous sa responsabilité dans le cadre du service. Cette politique doit prévoir une sauvegarde quotidienne de l'ensemble des données (informations, logiciels, configurations, etc.) sous la responsabilité du prestataire dans le cadre du service.

b) Le prestataire doit documenter et mettre en œuvre des mesures de protection des sauvegardes conformément à la politique de contrôle d'accès (voir chapitre 9). Cette politique doit prévoir une revue mensuelle des traces d'accès aux sauvegardes.

c) Le prestataire doit documenter et mettre en œuvre une procédure permettant de tester régulièrement la restauration des sauvegardes.

d) Le prestataire doit localiser les sauvegardes à une distance suffisante des équipements principaux en cohérence avec les résultats de l'appréciation de risques et permettant de faire face à des sinistres majeurs. Les sauvegardes sont assujetties aux mêmes exigences de localisation que les données opérationnelles. Le ou les sites de sauvegarde sont assujettis aux mêmes exigences de sécurité que le site principal, en particulier celles listées aux chapitres 8 et 11. Les communications entre site principal et site de sauvegarde doivent être protégées par chiffrement, conformément aux exigences du chapitre 10.

12.6. Journalisation des événements

a) Le prestataire doit documenter et mettre en œuvre une politique de journalisation incluant au minimum les éléments suivants :

- la liste des sources de collecte ;
- la liste des événements à journaliser par source ;
- l'objet de la journalisation par événement ;
- la fréquence de la collecte et base de temps utilisée ;
- la durée de rétention locale et centralisée ;
- les mesures de protection des journaux (dont chiffrement et duplication) ;
- la localisation des journaux.

b) Le prestataire doit générer et collecter les événements suivants :

- les activités des utilisateurs liées à la sécurité de l'information ;
- la modification des droits d'accès dans le périmètre de sa responsabilité ;
- les événements issus des mécanismes de lutte contre les codes malveillants (voir chapitre 12.4);
- les exceptions ;
- les défaillances ;
- tout autre événement lié à la sécurité de l'information.

c) Le prestataire doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires.

d) Le prestataire doit fournir, sur demande d'un commanditaire, l'ensemble des événements le concernant.

e) Il est recommandé que le système de journalisation mis en place par le prestataire respecte les recommandations de [NT_JOURNAL].

12.7. Protection de l'information journalisée

a) Le prestataire doit protéger les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité, conformément au chapitre 3.2 de [NT_JOURNAL].

b) Le prestataire doit gérer le dimensionnement de l'espace de stockage de l'ensemble des équipements hébergeant une ou plusieurs sources de collecte afin de permettre la conservation

locale des événements journalisés prévue par la politique de journalisation des événements. Cette gestion du dimensionnement doit prendre en compte les évolutions du système d'information.

c) Le prestataire doit transférer les événements journalisés en assurant leur protection en confidentialité et en intégrité, sur un ou plusieurs serveurs centraux dédiés et doit les stocker sur une machine physique distincte de celle qui les a générés.

d) Le prestataire doit mettre en place une sauvegarde des événements collectés suivant une politique adaptée.

e) Le prestataire doit exécuter les processus de journalisation et de collecte des évènements avec des comptes disposant de privilèges nécessaires et suffisants et doit limiter l'accès aux événements journalisés conformément à la politique de contrôle d'accès (voir chapitre 9.1).

12.8. Synchronisation des horloges

a) Le prestataire doit documenter et mettre en œuvre une synchronisation des horloges de l'ensemble des équipements sur une ou plusieurs sources de temps internes cohérentes entre elles. Ces sources pourront elles-mêmes être synchronisées sur plusieurs sources fiables externes, sauf pour les réseaux isolés.

b) Le prestataire doit mettre en place l'horodatage de chaque événement journalisé.

12.9. Analyse et corrélation des événements

a) Le prestataire doit documenter et mettre en œuvre une infrastructure permettant l'analyse et la corrélation des événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d'affecter la sécurité du système d'information du service, en temps réel ou *a posteriori* pour des événements remontant jusqu'à six mois.

b) Il est recommandé de s'appuyer sur le référentiel d'exigences des prestataires de détection d'incidents de sécurité [PDIS] pour la mise en place et l'exploitation de l'infrastructure d'analyse et de corrélation des événements.

c) Le prestataire doit acquitter les alarmes remontées par l'infrastructure d'analyse et de corrélation des événements au moins quotidiennement.

12.10. Installation de logiciels sur des systèmes en exploitation

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de contrôler l'installation de logiciels sur les équipements du système d'information du service.

b) Le prestataire doit documenter et mettre en œuvre une procédure de gestion de la configuration des environnements logiciels mis à la disposition du commanditaire, notamment pour leur maintien en condition de sécurité.

c) Le prestataire doit fournir une capacité d'inspection et de suppression, si nécessaire, des entrants (contrôle de l'authenticité et de l'innocuité des mises à jour, contrôle de l'innocuité des outils fournis, etc.) relatifs au périmètre de l'infrastructure technique :

- cette capacité d'inspection et de suppression doit générer des journaux d'activité et doit pouvoir faire l'objet d'un audit de code,
- les entrants doivent être traités sur des dispositifs spécifiques opérés et maintenus par le prestataire et hébergés dans une zone cloisonnée du reste de l'infrastructure.

12.11. Gestion des vulnérabilités techniques

a) Le prestataire doit documenter et mettre en œuvre un processus de veille permettant de gérer les vulnérabilités techniques des logiciels et des systèmes utilisés dans le système d'information du service.

b) Le prestataire doit évaluer son exposition à ces vulnérabilités en les incluant dans l'appréciation des risques et appliquer les mesures de traitement du risque adaptées.

12.12. Administration

a) Le prestataire doit documenter et mettre en œuvre une procédure obligeant les administrateurs sous sa responsabilité à utiliser des terminaux dédiés pour la réalisation exclusive des tâches d'administration, en accord avec le chapitre 4.1 intitulé « poste et réseau d'administration » de [NT_ADMIN]. Il doit les maîtriser et les maintenir à jour.

b) Le prestataire doit mettre en place des mesures de durcissement de la configuration des terminaux utilisés pour les tâches d'administration, notamment celles du chapitre 4.2 intitulé « sécurisation du socle » de [NT_ADMIN].

c) Lorsque le prestataire autorise une situation de mobilité pour les administrateurs sous sa responsabilité, il doit l'encadrer par une politique documentée. La solution mise en œuvre doit assurer que le niveau de sécurité de cette situation de mobilité est au moins équivalent au niveau de sécurité hors situation de mobilité (voir chapitres 9.6 et 9.7). Cette solution doit notamment inclure :

- l'utilisation d'un tunnel chiffré, non débrayable et non contournable, pour l'ensemble des flux (voir chapitre 10.2) ;
- le chiffrement intégral du disque (voir chapitre 10.1).

12.13. Télédiagnostic et télémaintenance des composants de l'infrastructure

a) Dans le cadre du télédiagnostic ou de la télémaintenance de composants de l'infrastructure, considérant les risques d'atteinte à la confidentialité des données des commanditaires, alors le prestataire doit :

- vérifier que la personne à qui l'accès doit être autorisé a satisfait aux vérifications de l'exigence 7.1.a relativement à la sensibilité ou à la spécificité des données du commanditaire ;
- vérifier que la personne à qui l'accès doit être autorisé est localisée au sein de l'Union Européenne ;
- dans le cas d'une intervention réalisée par une personne n'ayant pas satisfait aux vérifications de l'exigence 7.1.a, mettre en œuvre une passerelle sécurisée (poste de rebond) par laquelle la personne devra se connecter et permettant une supervision des actions (autorisation ou interdiction des actions, demande d'explications, etc..) en temps réel, par une personne ayant elle-même satisfait aux vérifications de l'exigence 7.1.a ;
- considérer les actions menées, une fois l'accès autorisé, comme des actions d'administration et les journaliser comme telles.
- supprimer l'autorisation d'accès à l'issue de l'intervention.

12.14. Surveillance des flux sortants de l'infrastructure

a) Le prestataire doit fournir une capacité d'inspection et de suppression des sortants de l'infrastructure technique relatifs au périmètre du service (informations de facturation, les éventuels journaux nécessaires au traitement d'incidents, etc.) :

- les sortants doivent pouvoir être expurgés des données pouvant porter atteinte à la confidentialité des données des commanditaires ;
- cette capacité d'inspection et de suppression doit générer des journaux d'activité et doit pouvoir faire l'objet d'un audit de code ;

- les sortants sont traités sur des dispositifs spécifiques opérés et maintenus par le prestataire, et hébergés dans une zone cloisonnée du reste de l'infrastructure.

13. Sécurité des communications

13.1. Cartographie du système d'information.

a) Le prestataire doit établir et tenir à jour une cartographie du système d'information du service, en lien avec l'inventaire des actifs (voir chapitre 8.1), comprenant au minimum les éléments suivants :

- la liste des ressources matérielles ou virtualisées ;
- les noms et fonctions des applications, supportant le service ;
- le schéma d'architecture réseau au niveau 3 du modèle OSI sur lequel les points névralgiques sont identifiés :
  - les points d'interconnexions, notamment avec les réseaux tiers et publics,
  - les réseaux, sous-réseaux, notamment les réseaux d'administration,
  - les équipements assurant des fonctions de sécurité (filtrage, authentification, chiffrement, etc.),
  - les serveurs hébergeant des données ou assurant des fonctions sensibles ;
- la matrice des flux réseau autorisés en précisant :
  - leur description technique (services, protocoles et ports) ;
  - la justification métier ou d'infrastructure technique ;
  - le cas échéant, lorsque des services, protocoles ou ports réputés non sûrs sont utilisés, les mesures compensatoires mises en place, dans la logique de défense en profondeur.

b) Le prestataire doit réviser au moins annuellement la cartographie.

13.2. Cloisonnement des réseaux

a) Le prestataire doit documenter et mettre en œuvre, pour le système d'information du service, les mesures de cloisonnement (logique, physique ou par chiffrement) pour séparer les flux réseau selon :

- la sensibilité des informations transmises ;
- la nature des flux (production, administration, supervision, etc.) ;
- le domaine d'appartenance des flux (des commanditaires – avec distinction par commanditaire ou ensemble de commanditaires, du prestataire, des tiers, etc.) ;
- le domaine technique (traitement, stockage, etc.).

b) Le prestataire doit cloisonner, physiquement ou par chiffrement, tous les flux de données internes au système d'information du service vis-à-vis de tout autre système d'information. Lorsque ce cloisonnement est réalisé par chiffrement, il est réalisé en accord avec les exigences du chapitre 10.2.

c) Dans le cas où le réseau d'administration de l'infrastructure technique ne fait pas l'objet d'un cloisonnement physique, les flux d'administration doivent transiter dans un tunnel chiffré, en accord avec les exigences du chapitre 10.2.

d) Le prestataire doit mettre en place et configurer un pare-feu applicatif pour protéger les interfaces d'administration destinées à ses commanditaires et exposées sur un réseau public.

e) Le prestataire doit mettre en œuvre sur l'ensemble des interfaces d'administration et de supervision de l'infrastructure technique du service un mécanisme de filtrage n'autorisant que les connexions légitimes identifiées dans la matrice des flux autorisés.

13.3. Surveillance des réseaux

a) Le prestataire doit disposer une ou plusieurs sondes de détection d'incidents de sécurité sur le système d'information du service. Ces sondes doivent notamment permettre la supervision de chacune des interconnexions du système d'information du service avec des systèmes d'information tiers et des réseaux publics. Ces sondes doivent être des sources de collecte pour l'infrastructure d'analyse et de corrélation des événements (voir chapitre 12.9).

14. Acquisition, développement et maintenance des systèmes d'information

14.1. Politique de développement sécurisé

a) Le prestataire doit documenter et mettre en œuvre des règles de développement sécurisé des logiciels et des systèmes, et les appliquer aux développements internes.

b) Le prestataire doit documenter et mettre en œuvre une formation adaptée en développement sécurisé aux employés concernés.

14.2. Procédures de contrôle des changements de système

a) Le prestataire doit documenter et mettre en œuvre une procédure de contrôle des changements apportés au système d'information du service.

b) Le prestataire doit documenter et mettre en œuvre une procédure de validation des changements apportés au système d'information du service sur un environnement de pré-production avant leur mise en production.

c) Le prestataire doit conserver un historique des versions des logiciels et des systèmes (développements internes ou externes, produits commerciaux) mis en œuvre pour permettre de reconstituer, le cas échéant dans un environnement de test, un environnement complet tel qu'il était mis en œuvre à une date donnée. La durée de conservation de cet historique doit être en accord avec celle des sauvegardes (voir chapitre 12.5).

14.3. Revue technique des applications après changement apporté à la plateforme d'exploitation

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de tester, préalablement à leur mise en production, l'ensemble des applications afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité du service.

14.4. Environnement de développement sécurisé

a) Le prestataire doit mettre en œuvre un environnement sécurisé de développement permettant de gérer l'intégralité du cycle de développement du système d'information du service.

b) Le prestataire doit prendre en compte les environnements de développement dans l'appréciation des risques et en assurer la protection conformément au présent référentiel.

14.5. Développement externalisé

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de superviser et de contrôler l'activité de développement externalisé des logiciels et des systèmes. Cette procédure doit s'assurer que l'activité de développement externalisé soit conforme à la politique de développement sécurisé du prestataire et permette d'atteindre un niveau de sécurité du développement externe équivalent à celui d'un développement interne (voir exigence 14.1 a).

14.6. Test de la sécurité et conformité du système

a) Le prestataire doit soumettre les systèmes d'information, nouveaux ou mis à jour, à des tests de conformité et de fonctionnalité de sécurité pendant le développement. Il doit documenter et mettre en œuvre une procédure de test qui identifie :

- les tâches à réaliser ;
- les données d'entrée ;

- les résultats attendus en sortie.

14.7. Protection des données de test

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'assurer l'intégrité des données de tests utilisés en pré-production.

b) Si le prestataire souhaite utiliser des données du commanditaire issues de la production pour réaliser des tests, le prestataire doit préalablement obtenir l'accord du commanditaire et les anonymiser. Le prestataire doit assurer la confidentialité des données lors de leur anonymisation.

15. Relations avec les tiers

15.1. Identification des tiers

a) Le prestataire doit tenir à jour une liste exhaustive des tiers participant à la mise en œuvre du service (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance, fournisseurs de climatisation, etc.). Cette liste doit préciser la contribution du tiers au service et au traitement des données à caractère personnel. Elle doit tenir compte des cas de sous-traitance à plusieurs niveaux.

b) Le prestataire doit tenir à disposition du commanditaire la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de sous-traitants au sens de l'article 28 du [RGPD] afin que le commanditaire puisse émettre des objections à cet égard.

15.2. La sécurité dans les accords conclus avec les tiers

a) Le prestataire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le prestataire doit inclure ces exigences dans les contrats conclus avec les tiers.

b) Le prestataire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent référentiel.

c) Le prestataire doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

15.3. Surveillance et revue des services des tiers

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences du présent référentiel, conformément au chapitre 18.3.

15.4. Gestion des changements apportés dans les services des tiers

a) Le prestataire doit documenter et mettre en œuvre une procédure de suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système d'information du service.

b) Dans la mesure où un changement de tiers participant à la mise en œuvre du service affecte le niveau de sécurité du service, le prestataire doit en informer l'ensemble des commanditaires sans délais conformément au chapitre 12.2 et mettre en œuvre les mesures permettant de rétablir le niveau de sécurité précédent.

15.5. Engagements de confidentialité

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.

16. Gestion des incidents liés à la sécurité de l'information

16.1. Responsabilités et procédures

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'apporter des réponses rapides et efficaces aux incidents de sécurité. Ces procédures doivent définir les moyens et délais de communication des incidents de sécurité à l'ensemble des commanditaires concernés ainsi que le niveau de confidentialité exigé pour cette communication.

b) Le prestataire doit informer ses employés et l'ensemble des tiers participant à la mise en œuvre du service de cette procédure.

c) Le prestataire doit documenter toute violation de données à caractère personnel et en informer son commanditaire. La violation doit être notifiée à la CNIL[1] si elle présente un risque pour les droits et libertés des personnes concernées. Elle doit faire l'objet d'une information auprès des personnes concernées lorsque le risque pour leur vie privée est élevé.

16.2. Signalements liés à la sécurité de l'information

a) Le prestataire doit documenter et mettre en œuvre une procédure exigeant de ses employés et des tiers 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.

b) Le prestataire doit documenter et mettre en œuvre une procédure permettant à l'ensemble des commanditaires de signaler tout incident de sécurité, avéré ou suspecté et toute faille de sécurité.

c) Le prestataire doit communiquer sans délai aux commanditaires les incidents de sécurité et les préconisations associées pour en limiter les impacts. Il doit permettre au commanditaire de choisir les niveaux de gravité des incidents pour lesquels il souhaite être informé.

d) Le prestataire doit communiquer les incidents de sécurité aux autorités compétentes conformément aux exigences légales et réglementaires en vigueur.

16.3. Appréciation des événements liés à la sécurité de l'information et prise de décision

a) Le prestataire doit apprécier les événements liés à la sécurité de l'information et décider s'il faut les qualifier en incidents de sécurité. Pour l'appréciation, il doit s'appuyer sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec le commanditaire.

Note : Les incidents de sécurité incluent les violations de données à caractère personnel.

b) Le prestataire doit utiliser une classification permettant d'identifier clairement les incidents de sécurité touchant des données relatives aux commanditaires, conformément aux résultats de l'appréciation des risques. Cette classification doit inclure les violations de données à caractère personnel.

16.4. Réponse aux incidents liés à la sécurité de l'information

a) Le prestataire doit traiter les incidents de sécurité jusqu'à leur résolution et doit informer les commanditaires conformément aux procédures.

1 Notification en ligne : https://notifications.cnil.fr/notifications/index

b) Le prestataire doit archiver les documents détaillant les incidents de sécurité.

c) Il est recommandé que le prestataire fasse appel à un prestataire de réponse aux incidents de sécurité [PRIS] qualifié pour traiter les incidents de sécurité nécessitant une expertise supplémentaire.

16.5. Tirer des enseignements des incidents liés à la sécurité de l'information

a) Le prestataire doit documenter et mettre en œuvre un processus d'amélioration continue afin de diminuer l'occurrence et l'impact de types d'incidents de sécurité déjà traités.

16.6. Recueil de preuves

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'enregistrer les informations relatives aux incidents de sécurité et pouvant servir d'éléments de preuve.

17. Continuité d'activité

17.1. Organisation de la continuité d'activité

a) Le prestataire doit documenter et mettre œuvre un plan de continuité d'activité prenant en compte la sécurité de l'information.

b) Le prestataire doit réviser annuellement le plan de continuité d'activité du service et à chaque changement majeur pouvant avoir un impact sur le service.

17.2. Mise en œuvre de la continuité d'activité

a) Le prestataire doit documenter et mettre en œuvre des procédures permettant de maintenir ou de restaurer l'exploitation du service et d'assurer la disponibilité des informations au niveau et dans les délais pour lesquels le prestataire s'est engagé vis-à-vis du commanditaire dans la convention de service.

17.3. Vérifier, revoir et évaluer la continuité d'activité

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de tester le plan de continuité d'activités afin de s'assurer qu'il est pertinent et efficace en situation de crise.

17.4. Disponibilité des moyens de traitement de l'information

a) Le prestataire doit documenter et mettre en œuvre les mesures qui lui permettent de répondre au besoin de disponibilité du service défini dans la convention de service (voir chapitre 19.1).

17.5. Sauvegarde de la configuration de l'infrastructure technique

a) Le prestataire doit documenter et mettre en œuvre une procédure de sauvegarde hors-ligne de la configuration de l'infrastructure technique.

17.6. Mise à disposition d'un dispositif de sauvegarde des données du commanditaire

a) Le prestataire doit documenter et mettre à disposition du commanditaire un service de sauvegarde de ses données.

18. Conformité

18.1. Identification de la législation et des exigences contractuelles applicables

a) Le prestataire doit identifier les exigences légales, réglementaires et contractuelles en vigueur applicables au service. En France, le prestataire doit considérer au minimum les textes suivants :

- les données à caractère personnel [LOI_IL], [RGPD] ;
- le secret professionnel [CP_ART_226_13], le cas échéant sans préjudice de l'application de l'article 40 alinéa 2 du Code de procédure pénale relatif au signalement à une autorité judiciaire ;
- l'abus de confiance [CP_ART_314-1] ;
- le secret des correspondances privées [CP_ART_226-15] ;
- l'atteinte à la vie privée [CP_ART_226-1] ;
- l'accès ou le maintien frauduleux à un système d'information [CP_ART_323-1].

b) Le prestataire doit, selon son rôle dans les traitements de données à caractère personnel (responsable de traitement, sous-traitant ou co-responsable) justifier et documenter les choix de mesures techniques et organisationnelles réalisés en vue de répondre aux exigences de protection des données à caractère personnel du présent référentiel (voir partie 19.5).

c) Le prestataire doit documenter et mettre en œuvre les procédures permettant de respecter les exigences légales, réglementaires et contractuelles en vigueur applicables au service, ainsi que les besoins de sécurité spécifiques (voir exigence 8.3b)).

d) Le prestataire doit, sur demande d'un commanditaire, lui rendre accessible l'ensemble de ces procédures.

e) Le prestataire doit documenter et mettre en œuvre un processus de veille actif des exigences légales, réglementaires et contractuelles en vigueur applicables au service.

18.2. Revue indépendante de la sécurité de l'information

18.2.1. Revue continue

a) Le prestataire doit documenter et mettre en œuvre un programme d'audit sur trois ans définissant le périmètre et la fréquence des audits en accord avec la gestion du changement, les politiques, et les résultats de l'appréciation des risques.

Le prestataire doit inclure dans le programme d'audit un audit qualifié par an réalisé par un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié. L'ensemble du programme d'audit doit notamment couvrir :

- l'audit de la configuration de l'infrastructure technique du service. Cet audit est réalisé par échantillonnage et doit inclure tous types d'équipements et de serveurs présents dans le système d'information du service ;
- le test d'intrusion des interfaces d'administration exposées sur un réseau public ;
- le test d'intrusion de l'interface utilisateur pour les services SaaS ;
- si le service bénéficie de développements internes, l'audit de code source portant sur les fonctionnalités de sécurité implémentées (l'approche en continue doit être privilégiée).

b) Il est recommandé que le prestataire mette en œuvre des mécanismes automatisés d'audit de la configuration adaptés à l'infrastructure technique du service.

18.2.2. Revue initiale

a) Préalablement à l'évaluation pour qualification du service, le prestataire doit faire réaliser une revue indépendante initiale de la sécurité de l'information par un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié. Cette revue initiale doit notamment couvrir[2] :

- pour les services autres que IaaS (CaaS, PaaS, SaaS, etc.), un audit de la configuration des ressources virtuelles ou physiques, des systèmes d'exploitation et logiciels de base (OS, middlewares, bases de données,...) dans le périmètre du service ;
- un test d'intrusion portant sur les interfaces d'administration du service mises à disposition des commanditaires;
- pour un service de type SaaS, un test d'intrusion portant sur l'interface mise à disposition des utilisateurs finaux ainsi qu'un audit du code source portant sur les fonctionnalités de sécurité implémentées (authentification, gestion des sessions, gestion du cloisonnement en cas de mode multi-tenant). Si le SaaS rend un service de sécurité de l'information, une certification[3] produit dédiée est nécessaire.

18.2.3. Revue des changements majeurs

a) En cas de changement majeur pouvant affecter le service, le prestataire doit faire réaliser une revue indépendante de changement par un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié. Cette revue indépendante de changement doit couvrir en particulier les activités d'audit suivantes :

- audit d'architecture ;
- audit organisationnel et physique ;
- audit de la configuration de l'infrastructure technique du service ;
- un test d'intrusion portant sur les interfaces d'administration du service mises à disposition des commanditaires;
- pour un service de type SaaS, un test d'intrusion portant sur l'interface mise à disposition des utilisateurs finaux ainsi qu'un audit du code source portant sur les fonctionnalités de sécurité implémentées (authentification, gestion des sessions, gestion du cloisonnement en cas de mode multi-tenant). Si le SaaS rend un service de sécurité de l'information, une certification[4] produit dédiée est nécessaire.

18.3. Conformité avec les politiques et les normes de sécurité

a) Le prestataire via le responsable de la sécurité de l'information doit s'assurer régulièrement de l'exécution correcte de l'ensemble des procédures de sécurité placées sous sa responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.

2 L'audit d'architecture, de la sécurité physique et de l'organisation de la sécurité de l'information n'est pas utile dans le cadre de la revue initiale car traité par ailleurs dans le référentiel.

3 La délivrance du certificat est subordonnée à la correction des vulnérabilités critiques identifiées lors de la revue initiale.

18.4. Examen de la conformité technique

a) Le prestataire doit documenter et mettre en œuvre une politique permettant de vérifier la conformité technique du service aux exigences du présent référentiel. Cette politique doit définir les objectifs, méthodes, fréquences, résultats attendus et mesures correctrices.

19. Exigences supplémentaires

19.1. Convention de service

a) Le prestataire doit établir une convention de service avec chacun des commanditaires du service. Toute modification de la convention de service doit être soumise à acceptation du commanditaire.

b) Le prestataire doit identifier dans la convention de service :

- les obligations, droits et responsabilités de chacune des parties : prestataire et tiers impliqués dans la fourniture du service, commanditaires, etc. ;
- les éléments explicitement exclus des responsabilités du prestataire dans la limite de ce que prévoient les exigences légales et réglementaires en vigueur, notamment l'article 28 du [RGPD] ;
- la localisation du service. La localisation du support doit être précisée lorsqu'il est réalisé depuis un Etat hors l'Union Européenne, comme le permet l'exigence 19.2.e.

c) Le prestataire doit proposer une convention de service appliquant le droit d'un État membre de l'Union Européenne. Le droit applicable doit être identifié dans la convention de service.

d) La convention de service doit indiquer que la collecte, la manipulation et le stockage des données faits dans le cadre de l'avant-vente, de la mise en œuvre, de la maintenance et l'arrêt du service sont conformes aux exigences édictées par la législation française et européenne en vigueur et que ces mêmes données ne sont pas soumises à d'autres régimes juridiques.

e) Le prestataire doit décrire dans la convention de service les moyens techniques et organisationnels qu'il met en œuvre pour assurer le respect du droit applicable.

f) Le prestataire doit inclure dans la convention de service une clause de révision de la convention prévoyant notamment une résiliation sans pénalité pour le commanditaire en cas de perte de la qualification octroyée au service.

g) Le prestataire doit inclure dans la convention de service une clause de réversibilité permettant au commanditaire de récupérer l'ensemble de ses données (fournies directement par le commanditaire ou produites dans le cadre du service à partir des données ou des actions du commanditaire).

h) Le prestataire doit assurer cette réversibilité via l'une des modalités techniques suivantes :

- la mise à disposition de fichiers suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le prestataire ;
- la mise en place d'interfaces techniques permettant l'accès aux données suivant un schéma documenté et exploitable (API, format pivot, etc.).

Les modalités techniques de la réversibilité figurent dans la convention de service.

i) Le prestataire doit indiquer dans la convention de service le niveau de disponibilité du service.

j) Le prestataire doit indiquer dans la convention de service qu'il ne peut disposer des données transmises et générées par le commanditaire, leur disposition étant réservée au commanditaire.

k) Le prestataire doit indiquer dans la convention de service qu'il ne divulgue aucune information relative à la prestation à des tiers, sauf autorisation formelle et écrite du commanditaire.

l) Le prestataire doit indiquer dans la convention de service si les données du commanditaire sont automatiquement sauvegardées ou non. Dans la négative, le prestataire doit sensibiliser le commanditaire aux risques encourus et clairement indiquer les opérations à mener par le commanditaire pour que ses données soient sauvegardées.

m) Le prestataire doit indiquer dans la convention de service s'il autorise l'accès distant pour des actions d'administration ou de support au système d'information du service.

n) Le prestataire doit préciser dans la convention de service que :

- le service est qualifié et inclure l'attestation de qualification ;
- le commanditaire peut déposer une réclamation relative au service qualifié auprès de l'ANSSI ;
- le commanditaire autorise l'ANSSI et l'organisme de qualification à auditer le service et son système d'information du service afin de vérifier qu'ils respectent les exigences du présent référentiel.

o) Le prestataire doit préciser dans la convention de service que le commanditaire autorise, conformément au présent référentiel (voir chapitre 18.2, un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié mandaté par le prestataire à auditer le service et son système d'information dans le cadre du plan de contrôle.

p) Le prestataire doit préciser dans la convention de service qu'il s'engage à mettre à disposition toutes les informations nécessaires à la réalisation d'audits de conformité aux dispositions de l'article 28 du [RGPD], menés par le commanditaire ou un tiers mandaté.

q) Il est recommandé que le tiers mandaté pour les audits soit un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié.

19.2. Localisation des données

a) Le prestataire doit documenter et communiquer au commanditaire la localisation du stockage et du traitement des données de ce dernier.

b) Le prestataire doit stocker et traiter les données du commanditaire au sein de l'Union Européenne.

c) Les opérations d'administration et de supervision du service doivent être réalisées depuis l'Union Européenne.

d) Le prestataire doit stocker et traiter les données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, données manipulées par le Software Defined Network, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) au sein de l'Union Européenne.

e) Le prestataire peut réaliser des opérations de support aux commanditaires depuis un État hors de l'Union Européenne. Il doit documenter la liste des opérations qui peuvent être effectuées par le support au commanditaire depuis un État hors de l'Union Européenne, et les mécanismes permettant d'en assurer le contrôle d'accès et la supervision depuis l'Union Européenne.

19.3. Régionalisation.

a) Le prestataire doit s'assurer que les interfaces du service accessibles au commanditaire soient au moins disponibles en langue française.

b) Le prestataire doit fournir un support de premier niveau en langue française.

19.4. Fin de contrat

a) À la fin du contrat liant le prestataire et le commanditaire, que le contrat soit arrivé à son terme ou pour toute autre cause, le prestataire doit assurer un effacement sécurisé de l'intégralité des données du commanditaire. Cet effacement doit faire l'objet d'un préavis formel au commanditaire de la part du prestataire respectant un délai de vingt et un jours calendaires. L'effacement peut être réalisé suivant l'une des méthodes suivantes, et ce dans un délai précisé dans la convention de service :

- effacement par réécriture complète de tout support ayant hébergé ces données ;
- effacement des clés utilisées pour le chiffrement des espaces de stockage du commanditaire décrit au chapitre 10.1 ;
- recyclage sécurisé, dans les conditions énoncées au chapitre 11.9.

b) À la fin du contrat, le prestataire doit supprimer les données techniques relatives au commanditaire (annuaire, certificats, configuration des accès, etc.).

19.5. Protection des données à caractère personnel

a) Le prestataire doit justifier du respect des principes de protection des données pour les traitements de données à caractère personnel mis en œuvre pour son propre compte. Il doit justifier au minimum les points suivants :

- les finalités des traitements déterminées, explicites et légitimes ;
- la traçabilité des activités de traitement pour son compte et celui de son commanditaire ;
- le fondement licite des traitements ;
- l'interdiction du détournement de finalité des traitements ;
- les données utilisées respectent le principe du minimum nécessaire et suffisant pour les traitements ; ainsi sont adéquates, pertinentes et limitées ;
- la qualité des données utilisées pour les traitements maintenue : données exactes et tenues à jour ;
- les durées de conservation définies et limitées.

b) Le prestataire doit justifier, pour les traitements de données à caractère personnel mis en œuvre pour son propre compte, du respect des droits des personnes concernées. Il doit justifier au minimum les points suivants :

- l'information des usagers via un traitement loyal et transparent ;
- le recueil du consentement des usagers : exprès, démontrable et retirable ;
- la possibilité pour les usagers d'exercer les droits d'accès, de rectification et d'effacement ;
- la possibilité pour les usagers d'exercer les droits de limitation du traitement, de portabilité et d'opposition.

c) Lorsqu'il agit en qualité de sous-traitant au sens de l'article 28 de [RGPD], le prestataire doit apporter assistance et conseil au commanditaire en l'informant si une instruction de ce dernier constitue une violation des règles de protection des données.

19.6. Immunité au droit extracommunautaire

a) Le siège statutaire, administration centrale ou principal établissement du prestataire doit être établi au sein d'un Etat membre de l'Union européenne.

b) Le capital social et les droits de vote dans la société du prestataire ne doivent pas être, directement ou indirectement :

- individuellement détenus à plus de 24% ;
- et collectivement détenus à plus de 39% ;

par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un Etat non membre de l'Union européenne.

Ces entités tierces susmentionnées ne peuvent pas individuellement :

- en vertu d'un contrat ou de clauses statutaires, disposer d'un droit de véto ;
- en vertu d'un contrat ou de clauses statutaires, désigner la majorité des membres des organes d'administration, de direction ou de surveillance du prestataire.

c) En cas de recours par le prestataire, dans le cadre des services fournis au commanditaire, aux services d'une société tierce - y compris un sous-traitant - possédant son siège statutaire, administration centrale ou principal établissement au sein d'un Etat non membre de l'Union européenne ou appartenant ou étant contrôlée par une société tierce domiciliée en dehors l'Union européenne, cette susdite société tierce ne doit ni avoir la compétence pratique d'obtenir les données opérées au travers du service. Ces données visées sont celles qui sont confiées au prestataire par les commanditaires ainsi que toutes données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, données manipulées par le Software Defined Network, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) comprenant des informations sur les commanditaires.

Pour les besoins du présent article, la notion de contrôle est entendue comme étant celle mentionnée au II de l'article L233-3 du Code de commerce.

d) Dans le cadre du paragraphe 3, toute société tierce à laquelle le prestataire recourt pour fournir tout ou partie du service rendu au commanditaire, doit garantir au prestataire une autonomie d'exploitation continue dans la fourniture des services d'informatique en nuage qu'il opère ou doit être qualifié SecNumCloud.

Pour les besoins du présent article, la notion d'autonomie d'exploitation est entendue comme étant la capacité de maintenir la fourniture du service d'informatique en nuage en faisant appel aux compétences propres du prestataire ou en recourant à des prestations disponibles auprès d'au moins deux sociétés tierces.

e) Le service fourni par le prestataire doit respecter la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit. Il peut être pris en considération pour l'appréciation de la conformité susmentionnée, le fait que le prestataire entretienne des liens avec un gouvernement ou un organisme public étrangers[4].

[4] *formulation reprise de l'article R151-10 du code monétaire et financier sur le sujet du contrôle des investissements étrangers en France.*

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponible sur http://www.legifrance.gouv.fr
[RGPD]	Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible sur https://eur-lex.europa.eu
[CP_ART_314-1]	Article 334-1 du Code pénal relatif à l'abus de confiance. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-1]	Article 226-1 du Code pénal relatif à l'atteinte à la vie privée. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-13]	Article 226-13 du Code pénal relatif au secret professionnel. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-15]	Article 226-15 du Code pénal relatif au secret des correspondances. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_323-1]	Article 323-1 du Code pénal relatif à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données. Disponible sur http://www.legifrance.gouv.fr
[IGI_1300]	Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale. Disponible sur http://www.legifrance.gouv.fr
[II_910]	Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, 22 octobre 2013. Disponible sur http://www.legifrance.gouv.fr
[PSSIE]	Politique de sécurité des systèmes d'information de l'État (PSSIE), portée par la circulaire du Premier ministre n°5725/SG du 17 juillet 2014. Disponible sur http://www.legifrance.gouv.fr

II. Normes et documents techniques

Renvoi	Document
[EX_DONNEES]	Documents d'exigences complémentaires applicables aux prestataires d'informatique en nuage souhaitant héberger des données relevant d'une réglementation spécifique, ANSSI, version en vigueur. Disponibles sur http://www.ssi.gouv.fr
[CRYPTO_B1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[CRYPTO_B2]	Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[NT_IPSEC]	Recommandations de sécurité relatives à IPsec, note technique n° DAT-NT-003/ANSSI/SDE/NP du 3 août 2015, ANSSI. Disponible sur http://www.ssi.gouv.fr

Renvoi	Document
[NT_TLS]	Recommandations de sécurité relatives à TLS, note technique n° SDE-NT-35/ANSSI/SDE/NP du 19 août 2016, ANSSI. Disponible sur http://www.ssi.gouv.fr
[NT_SSH]	Recommandations pour un usage sécurisé d'(Open)SSH, note technique n° DAT-NT-007/ANSSI/SDE/NP du 17 août 2015, ANSSI. Disponible sur http://www.ssi.gouv.fr
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI. Disponible sur http://www.ssi.gouv.fr
[NT_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, Guide ANSSI n° ANSSI-PA-022 du 11 mai 2021, ANSSI Disponible sur http://www.ssi.gouv.fr
[NT_MDP]	Recommandations relatives à l'authentification multifacteur et aux mots de passe, Guide ANSSI n° ANSSI-PG-078 du 8 octobre 2021, ANSSI Disponible sur http://www.ssi.gouv.fr
[G_SANSCONTACT]	Guide de sécurité des technologies sans contact pour le contrôle des accès physiques, guide du 19 novembre 2012, ANSSI Disponible sur http://www.ssi.gouv.fr
[PASSI]	Référentiel d'exigences applicables à un prestataire d'audit de la sécurité des systèmes d'information, ANSSI, version en vigueur Disponible sur http://www.ssi.gouv.fr
[PDIS]	Référentiel d'exigences applicables à un prestataire de détection des incidents de sécurité, ANSSI, version en vigueur Disponible sur http://www.ssi.gouv.fr
[PRIS]	Référentiel d'exigences applicables à un prestataire de réponse aux incidents de sécurité, ANSSI, version en vigueur Disponible sur http://www.ssi.gouv.fr
[ISO27001]	Norme internationale ISO/IEC 27001:2013 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences. Disponible sur http://www.iso.org

III. Autres références documentaires

Renvoi	Document
[PROCESS_QUALIF]	Processus de qualification d'un service, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[GUIDE_CNIL]	Recommandations pour les entreprises qui envisagent de souscrire à des services de cloud computing. Disponible sur https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services

Annexe 2 Recommandations aux commanditaires

Cette annexe liste les recommandations de l'ANSSI aux commanditaires de prestations d'informatique en nuage.

a) Le commanditaire peut, lorsqu'il est une autorité administrative ou un opérateur d'importance vitale, demander à l'ANSSI de participer à la définition du cahier des charges faisant l'objet d'un appel d'offres ou d'un contrat.

b) Il est recommandé que le commanditaire choisisse son prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'ANSSI, la qualification d'un prestataire d'informatique en nuage attestant de sa conformité à l'ensemble des exigences du présent référentiel.

c) Pour bénéficier d'une prestation qualifiée, c'est-à-dire conforme à l'ensemble des exigences du présent référentiel, le commanditaire doit :

- choisir le prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'ANSSI ;
- exiger du prestataire de stipuler dans la convention de service que la prestation réalisée est une prestation qualifiée.

En effet, un prestataire qualifié garde la faculté de réaliser des prestations non qualifiées. Le recours à un prestataire issu du catalogue des prestataires qualifiés est donc une condition nécessaire mais pas suffisante pour bénéficier d'une prestation qualifiée, le commanditaire doit donc également exiger une prestation qualifiée.

d) Il est recommandé que le commanditaire utilise le guide d'achat des produits de sécurité et des services de confiance [GUIDE_ACHAT] qui a pour vocation à accompagner la fonction achat des commanditaires lors des appels d'offres.

e) Le commanditaire peut, conformément au processus de qualification des prestataires de service de confiance [PROCESS_QUALIF], déposer auprès de l'ANSSI une réclamation contre un prestataire qualifié pour lequel il estime que ce dernier n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée.

S'il s'avère après instruction de la réclamation que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, et selon la gravité, la qualification du prestataire peut être suspendue, retirée ou sa portée de qualification réduite.

f) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des informations classifiées de défense [IGI_1300]

g) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des articles contrôlés de la sécurité des systèmes d'information (ACSSI) [II_910].

h) La conformité du service du prestataire au référentiel SecNumCloud ne se substitue pas aux exigences légales ou réglementaires applicables à certaines données spécifiques telles que les données de niveau Diffusion Restreinte ou les données de santé. L'hébergement de données spécifiques dans un service qualifié SecNumCloud nécessite le respect d'exigences complémentaires décrites dans les documents [EX_DONNEES] à vérifier dans le cadre d'une démarche d'appréciation des risques de son propre SI par le commanditaire.

i) Pour l'accès aux interfaces de gestion du service, il est recommandé que le commanditaire utilise des moyens (terminaux, serveurs) dédiés aux tâches d'administration et conformes aux recommandations du guide [NT_ADMIN].