RÉFÉRENTIEL D'EXIGENCES CONCERNANT LA QUALIFICATION DES PRESTATAIRES D'INFORMATIQUE EN NUAGE ET D'HÉBERGEMENT (PINH) PRIS AU TITRE DU PARAGRAPHE C) DE L'ARTICLE 3 DE L'ORDONNANCE SOUVERAINE N° 5.664 DU 23 DÉCEMBRE 2015 CRÉANT L'AGENCE MONÉGASQUE DE SÉCURITÉ NUMÉRIQUE, MODIFIÉE

Annexe à l'Arrêté Ministériel n° 2018-1108
du 26 novembre 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.411

DU 7 DÉCEMBRE 2018

SOMMAIRE

Contenu

1. Introduction 4
1.1. Présentation générale....4
1.1.1. Contexte....4
1.1.2. Objet du document 4
1.2. Abréviations et définitions....5
1.2.1. Abréviations....5
1.2.2. Définitions 5
1.2.3. Définition des Rôles 6
2. Activités visées par le référentiel 7
2.1. Fourniture de services en mode SaaS 7
2.2. Fourniture de services en mode PaaS 7
2.3. Fourniture de services en mode IaaS 7
2.4. Fourniture de services d'hébergement 7
3. Qualification des prestataires d'informatique en nuage et d'hébergement....8
3.1. Modalités de la qualification 8
3.2. Portée de la qualification....8
3.3. Avertissements....8
3.3.1. Risques liés à l'absence de qualification ...8
3.3.2. Risques liés à la protection des informations....8
4. Niveaux de qualification....9
4.1. Niveau Essentiel....9
4.2. Niveau Avancé....9
5. Politiques de sécurité de l'information et gestion du risque 9
5.1. Principes 9
5.2. Politique de sécurité de l'information....9
5.3. Appréciation des risques....9
6. Organisation de la sécurité de l'information....10
6.1. Fonctions et responsabilités liées à la sécurité de l'information 10
6.2. Séparation des tâches 10
6.3. Relations avec les autorités 10
6.4. La sécurité de l'information dans la gestion de projet....10
7. Sécurité des ressources humaines 10
7.1. Sélection des candidats....10
7.2. Conditions d'embauche....10
7.3. Sensibilisation, apprentissage et formations à la sécurité 11
7.4. Processus disciplinaire 11
7.5. Rupture, terme ou modification du contrat de travail....11
8. Gestion des actifs 11
8.1. Inventaire et propriété des actifs 11
8.2. Restitution des actifs 11
8.3. Identification des besoins de sécurité de l'information 11
8.4. Marquage et manipulation de l'information....12
8.5. Gestion des supports amovibles....12
9. Contrôle d'accès et gestion des identités 12
9.1. Politiques et contrôle d'accès....12
9.2. Enregistrement et désinscription des utilisateurs....12
9.3. Gestion des droits d'accès....12
9.4. Revue des droits d'accès utilisateurs 13
9.5. Gestion des authentifications des utilisateurs....13
9.6. Accès aux interfaces d'administration 13
9.7. Restriction des accès à l'information....14

10. Cryptologie 14
10.1. Chiffrement des données stockées 14
10.2. Chiffrement des flux 14
10.3. Hachage des mots de passe 14
10.4. Non répudiation 14
10.5. Gestion des secrets 14
11. Sécurité physique et environnementale 15
11.1. Périmètres de sécurité physique 15
11.1.1. Zones publiques 15
11.1.2. Zones privées 15
11.1.3. Zones sensibles 15
11.2. Contrôle d'accès physique 15
11.2.1. Zones privées 15
11.2.2. Zones sensibles 15
11.3. Protection contre les menaces extérieures et environnementales 16
11.4. Travail dans les zones privées et sensibles 16
11.5. Zones de livraison et de chargement 16
11.6. Sécurité du câblage 16
11.7. Maintenance des matériels 16
11.8. Sortie des actifs 17
11.9. Recyclage sécurisé du matériel 17
11.10. Matériel en attente d'utilisation 17
12. Sécurité liée à l'exploitation 17
12.1. Procédures d'exploitation documentées 17
12.2. Gestion des changements 17
12.3. Séparation des environnements de développement, de test et d'exploitation 17
12.4. Mesures contre les codes malveillants 17
12.5. Sauvegarde des informations 17
12.6. Journalisation des événements 18
12.7. Protection de l'information journalisée 18
12.8. Synchronisation des horloges 18
12.9. Analyse et corrélation des événements 18
12.10. Installation de logiciels sur des systèmes en exploitation 19
12.11. Gestion des vulnérabilités techniques 19
12.12. Administration 19
13. Sécurité des communications 19
13.1. Cartographie du système d'information 19
13.2. Cloisonnement des réseaux 19
13.3. Surveillance des réseaux 20
14. Acquisition, développement et maintenance des systèmes d'information 20
14.1. Politique de développement sécurisé 20
14.2. Procédures de contrôle des changements de système 20
14.3. Revue technique des applications après changement apporté à la plateforme d'exploitation 20
14.4. Environnement de développement sécurisé 20
14.5. Développement externalisé 20
14.6. Test de la sécurité et conformité du système 20
14.7. Protection des données de test 21
15. Relations avec les tiers 21
15.1. Identification des tiers 21
15.2. La sécurité dans les accords conclus avec les tiers 21
15.3. Surveillance et revue des services des tiers 21
15.4. Gestion des changements apportés dans les services des tiers 21
15.5. Engagements de confidentialité 21
16. Gestion des incidents liés à la sécurité de l'information 21
16.1. Responsabilités et procédures 21
16.2. Signalements liés à la sécurité de l'information ou physique 21

16.3. Appréciation des événements liés à la sécurité de l'information ou physique et prise de décision.....22

16.4. Réponse aux incidents liés à la sécurité de l'information ou physique.....22

16.5. Enseignements tirés des incidents liés à la sécurité de l'information ou physique.....22

16.6. Recueil de preuves 22

17. Continuité d'activité 22

17.1. Organisation de la continuité d'activité 22

17.2. Mise en œuvre de la continuité d'activité.....22

17.3. Vérification, révision et évaluation de la continuité d'activité 22

17.4. Disponibilité des moyens de traitement de l'information.....22

18. Conformité.....22

18.1. Identification de la législation et des exigences contractuelles applicables.....22

18.2. Revue indépendante de la sécurité de l'information 23

18.3. Conformité avec les politiques et les normes de sécurité 23

18.4. Examen de la conformité technique.....23

19. Exigences supplémentaires.....23

19.1. Convention de service 23

19.2. Localisation des données.....24

19.3. Régionalisation 24

19.4. Fin de contrat.....24

Appendice 1 Références documentaires.....25

I. Codes, textes législatifs et réglementaires 25

II. Normes et documents techniques 25

Appendice 2 Recommandations aux commanditaires.....27

1. Introduction

1.1. Présentation générale

1.1.1. Contexte

Le référentiel « Prestataire d'Informatique en Nuage et d'Hébergement » (PINH) a vocation à permettre la qualification des prestataires d'informatique en nuage (ou *cloud computing*) et d'hébergement.

Lesdits prestataires fournissent différents services habituellement classés en quatre types d'activité :

- infrastructure en tant que service (IaaS),
- plateforme en tant que service (PaaS),
- logiciel en tant que service (SaaS), et
- hébergement de matériel.

Ces activités sont précisées au sein du paragraphe 2.

Le présent référentiel suppose que la gestion de la sécurité de l'information, mise en place par le PINH, soit conforme à la norme internationale [ISO27001] dont il reprend d'ailleurs la structure de l'appendice A. Néanmoins, ce référentiel comporte des exigences additionnelles qui le différencient de ce standard existant et n'induisent pas l'équivalence entre les deux ensembles de règles.

1.1.2. Objet du document

Le référentiel PINH a pour but de traiter le problème de la sécurité de manière globale. Les prestataires disposent ainsi d'un cadre stable dans lequel s'inscrit la qualification. Les usagers peuvent ainsi fonder leur confiance sur cette qualification.

Il constitue donc le référentiel d'exigences applicables à un prestataire d'informatique en nuage et d'hébergement, ci-après dénommé le « prestataire ».

Le présent référentiel a vocation à permettre la qualification de cette famille de prestataires selon les modalités décrites au paragraphe 3.

Il permet aux clients du PINH 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.

Le présent référentiel n'exclut ni l'application de la législation et de la réglementation monégasques, 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.

Il 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 comme par exemple le simple hébergement de serveurs.

1.2. Abréviations et définitions

1.2.1. Abréviations

Les abréviations utilisées dans le présent référentiel sont :

AMSN	Agence Monégasque de Sécurité Numérique
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CCIN	Commission de Contrôle des Informations Nominatives
CSN	Confidentiel de Sécurité Nationale
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 d'Incident de Sécurité
PRIS	Prestataire de Réponse aux Incidents de Sécurité
PSSI-E	Politique de Sécurité des Systèmes d'Information de l'État
RGS	Référentiel Général de Sécurité
SaaS	Software as a Service

1.2.2. Définitions

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.

Client ou commanditaire - entité faisant appel à un prestataire d'informatique en nuage et d'hébergement.

***Cloud computing* (informatique en nuage) -** modèle permettant un accès aisé, à la demande et au travers d'un réseau, à un ensemble de ressources informatiques partagées ou non et configurables.

Commanditaire - toute entité souhaitant bénéficier d'une prestation d'informatique en nuage ou d'hébergement.

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.

IaaS - services d'informatique en nuage pour lequel on accède aux ressources informatiques dans un environnement virtualisé le « Cloud » à travers une connexion, généralement Internet. Dans le cas de l'IaaS, la ressource, le matériel informatique sont virtualisés. Le service peut inclure des offres telles que l'espace serveur, des connections réseau, la bande passante, les adresses IP.

Incident lié à la sécurité de l'information - un ou plusieurs événement(s) lié(s) 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.

Informatique en nuage - Voir *cloud computing*

Infrastructure technique - ensemble des composants matériels et logiciels nécessaires à la mise à disposition de ressources affectées à la demande (virtualisées ou non). Ce socle permet l'accomplissement de la prestation dans le cadre d'un service Infrastructure as a Service (IaaS) ou d'hébergement, ou sert de base à la construction du service dans les autres cas.

Interface d'administration - interface logicielle permettant à une entité disposant des privilèges requis (un administrateur, un compte de service, etc.) de réaliser des actions d'administration et de configuration 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.

PaaS - une Plateforme en tant que Service (PaaS) est un service d'informatique en nuage permettant aux entreprises d'externaliser l'hébergement des outils logiciels et matériels de développement d'applications.

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

Prestataire - organisme proposant un service d'informatique en nuage ou d'hébergement 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 conformément à l'arrêté ministériel n° 2017-625 du 16 août 2017.

Prestataire de détection d'incident de sécurité - organisme réalisant des prestations de détection d'incident de sécurité. Il est dit qualifié si un organisme d'évaluation de la conformité a attesté de la conformité au Référentiel d'exigences des prestataires de détection d'incident de sécurité et si le Directeur de l'AMSN a prononcé sa qualification.

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.

SaaS - le SaaS, ou Logiciel en tant que Service, est un modèle de distribution de logiciel(s) à travers l'informatique en nuage. Les applications sont hébergées par le fournisseur de service.

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).

Système d'information - est qualifié de système d'information, tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

Tiers - tout intervenant (personne physique ou morale) dans le service PINH autre que l'entité avec lequel a été conclu le service.

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

1.2.3. Définition des Rôles

Administrateur - toute personne ayant en charge le bon fonctionnement du système d'information et/ou disposant d'accès privilégiés et de droits spécifiques permettant de modifier des systèmes d'information, des réseaux, des applications, des infrastructures et/ou des postes de travail. Ces droits étendus, dont elle a besoin pour réaliser sa mission au niveau organisationnel ou technique peuvent permettre d'accéder aux données des utilisateurs ou des administrés de l'État liées au périmètre qu'il administre dans le cadre de sa mission.

Administrateur de sécurité - administrateur en charge de la configuration de sécurité, notamment de la gestion des droits d'accès des administrateurs.

Administrateur d'infrastructure - administrateur en charge de la gestion et du maintien en conditions opérationnelles et de sécurité de l'infrastructure technique du service. Il est toujours sous la responsabilité du prestataire.

Administrateur système - administrateur des ressources logiques supportées par l'infrastructure technique du service. Selon le type d'architecture du service, l'administration système peut concerner les ressources abstraites (machines virtuelles, réseaux virtuels, etc.), les systèmes d'exploitation, les intergiciels, les logiciels métier, etc. (voir le schéma du paragraphe 2).

Administrateur métier - administrateur en charge de l'administration fonctionnelle au niveau applicatif.

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 client dans le cas d'un service interne, ou de ses propres clients dans le cas d'un service proposé à l'extérieur.

Les rôles d'administrateurs peuvent être attribués, soit au prestataire, soit aux clients, soit partagés, cela en fonction du service et des responsabilités respectives décrites dans la convention de service.

2. Activités visées par le référentiel

2.1. Fourniture de services en mode SaaS

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

2.2. Fourniture de services en mode PaaS

Ce mode concerne la mise à disposition par le prestataire de plateformes d'hébergement d'applications. Le client n'a pas la maîtrise de l'infrastructure technique sous-jacente, gérée et contrôlée par le prestataire (réseau, serveurs, systèmes d'exploitation [OS], stockage, etc.). Le client 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.

2.3. Fourniture de services en mode IaaS

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

2.4. Fourniture de services d'hébergement

Ce service concerne la mise à disposition de locaux avec l'énergie, la climatisation et la sécurité d'accès aux locaux. Selon la décision du client, le prestataire peut fournir d'autres matériels comme les baies informatiques, le contrôle d'accès aux baies ou au local ou sous local, les réseaux, les gestes de proximité, etc. sans qu'aucun des services prévus aux paragraphes 2.1 à 2.3 ci-dessus ne soient fournis.

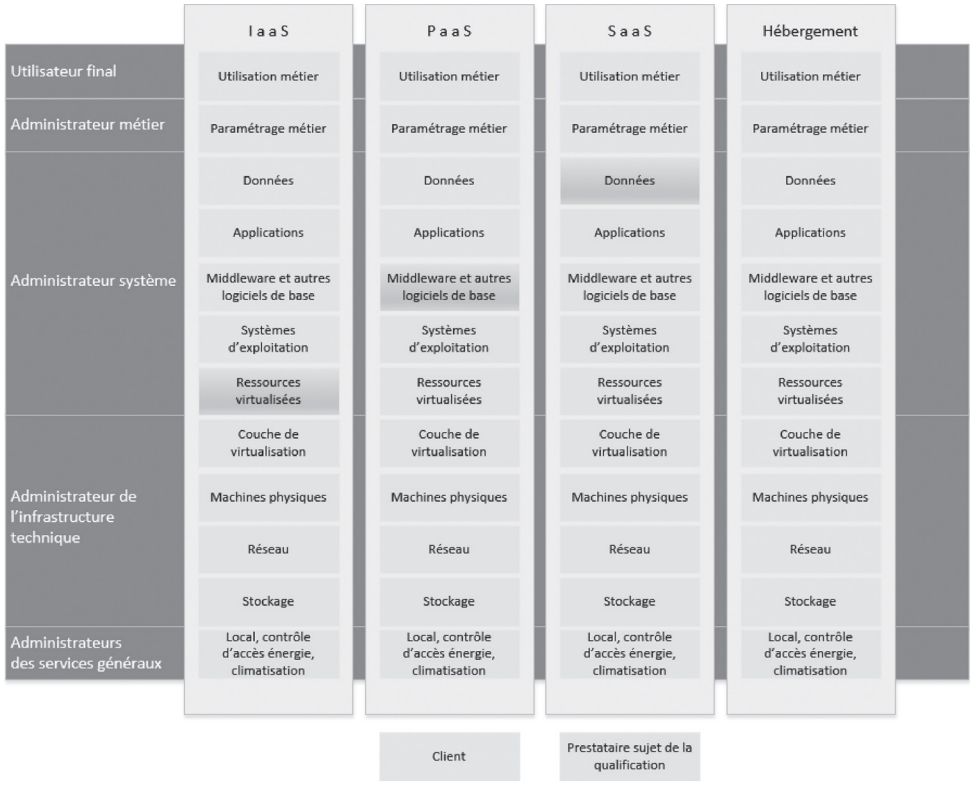

Figure 1 - Répartition des responsabilités par type de service

3. Qualification des prestataires d'informatique en nuage et d'hébergement

3.1. Modalités de la qualification

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

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

La qualification des prestataires est réalisée par le Directeur de l'Agence Monégasque de Sécurité Numérique conformément à l'article 3 de l'Ordonnance Souveraine n° 2015-5664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée, et selon le processus suivant, qui permet d'attester de la conformité du prestataire aux exigences du référentiel :

a) Le respect des exigences du référentiel par les prestataires d'audit est vérifié par un organisme de certification accrédité par le comité français d'accréditation (COFRAC) et habilité par l'Agence Monégasque de Sécurité Numérique. La liste des organismes de certification est disponible et téléchargeable sur le site de l'Agence Monégasque de Sécurité Numérique.

b) La qualification est attribuée, pour une durée maximale de trois ans, aux prestataires par le Directeur de l'Agence Monégasque de Sécurité Numérique au regard du rapport émis par l'organisme de certification et après délivrance du certificat par ce dernier.

c) Un audit de surveillance annuel est réalisé par un organisme de certification après la décision de qualification.

Pour les prestataires déjà qualifiés en France par l'ANSSI, le Directeur de l'Agence Monégasque de Sécurité Numérique peut prononcer leur qualification au niveau essentiel pour la Principauté.

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 paragraphe 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 d'informatique en nuage et d'hébergement 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 d'informatique en nuage et d'hébergement 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 PINH ne se substitue pas aux exigences légales ou réglementaires applicables à certaines données spécifiques telles que les données de santé, les données protégées par la mention particulière Diffusion Restreinte (dites données sensibles) et les données classifiées de sécurité nationale, au sens de l'arrêté ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié. L'hébergement de données spécifiques dans un service qualifié PINH peut nécessiter le respect d'exigences complémentaires.

Les clauses dudit 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 client, mais n'apporte pas de garanties techniques fortes contre un accès du prestataire aux données traitées sur le système d'information du service. Il permet au mieux de garantir les engagements contractuels. Les clients 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. Niveaux de qualification

On distingue deux niveaux de qualification des services d'informatique en nuage et d'hébergement :

4.1. Niveau Essentiel

Le Niveau Essentiel permet le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence limitée pour le client.

Il assure notamment le respect des bonnes pratiques de sécurité relevant de l'hygiène informatique telles que décrites dans le guide d'hygiène informatique [HYGIENE] de l'ANSSI.

Les exigences pour le Niveau Essentiel sont définies ci-après dans le présent référentiel.

La conformité d'un service d'informatique en nuage ou d'hébergement au Niveau Essentiel n'atteste pas de sa conformité à la Politique de Sécurité des Systèmes d'Information de l'État.

4.2. Niveau Avancé

Le Niveau Avancé permet le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence importante pour le client, voire pourrait mettre en péril sa pérennité.

Les exigences pour le Niveau Avancé sont celles du Niveau Essentiel avec en plus l'obligation :

- que le service soit effectué sur le territoire de la Principauté, avec garantie qu'aucune information d'administration et de supervision ne puisse sortir du territoire ;

- que le stockage des données soit effectué sur le territoire de la Principauté, sans aucune possibilité de sortie ;

- que certaines recommandations, précisées ci-après, du Niveau Essentiel deviennent des obligations ;

- que la prestation réalisée par le PINH soit conforme à la Politique de Sécurité des Systèmes d'Information de l'État.

Le Niveau Avancé est obligatoire pour les données sensibles de l'État et des établissements publics.

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 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 ; quand le commanditaire est l'État, le prestataire doit appliquer la PSSI-E.

b) La politique de sécurité de l'information doit identifier les engagements du prestataire quant au respect de la législation et de la réglementation en vigueur selon la nature des informations qui pourraient être confiées par le client au prestataire ; il revient en revanche *in fine* au client 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 paragraphes 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 régulièrement la politique de sécurité de l'information et à chaque changement majeur pouvant avoir un impact sur le service.

5.3. Appréciation des risques

1. Le prestataire doit réaliser et documenter une analyse des risques couvrant l'ensemble du périmètre du service.

2. Le prestataire doit réaliser ladite analyse de risques en utilisant une méthode documentée garantissant la reproductibilité et la comparabilité de la démarche.

3. Le prestataire doit prendre en compte dans l'analyse des risques :

- la gestion d'informations client ayant des besoins de sécurité différents ;

- les risques de défaillance des mécanismes de cloisonnement des ressources de l'infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les clients ;

- les risques liés à l'effacement incomplet des données stockées sur les espaces de mémoire ou de stockage partagés entre clients, en particulier lors des réallocations des espaces de mémoire et de stockage ;

- les risques d'accès aux matériels permettant la gestion technique centralisée (climatisation, énergie, …) du service d'hébergement ;

- les risques liés à l'exposition des interfaces d'administration sur un réseau public.

4. Lorsqu'il existe des exigences légales, réglementaires ou sectorielles spécifiques liées aux types d'informations confiées par le client au prestataire, ce dernier doit les prendre en compte dans son analyse 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.

5. La direction du prestataire doit accepter formellement les risques résiduels identifiés dans l'analyse des risques.

6. Le prestataire doit réviser annuellement l'analyse 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 et de la sécurité physique 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 et de sécurité physique 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 et de sécurité physique est toujours pertinente.

6.2. Séparation des tâches

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

Il est recommandé (obligatoire pour le Niveau Avancé), que le prestataire mette en place des relations appropriées avec l'Agence Monégasque de Sécurité Numérique et la Commission de Contrôle des Informations Nominatives, ainsi que, le cas échéant, avec les autorités sectorielles selon la nature des informations confiées par le client au prestataire.

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

a) Le prestataire doit documenter une analyse des risques, sur le périmètre du projet, préalablement à sa réalisation 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 client 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

Le prestataire doit documenter et mettre en œuvre une procédure de vérification des informations concernant son personnel conforme aux lois et règlements en vigueur. Celle-ci doit prévoir notamment de demander aux candidats à un recrutement un extrait du bulletin n° 3 du casier judiciaire datant de moins de 3 mois.

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

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 ;

- 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 client ;

- 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 nationales en vigueur et les bonnes pratiques liées à leurs activités.

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

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

7.3. Sensibilisation, apprentissage et formations à la sécurité

a) Le prestataire doit sensibiliser l'ensemble des personnels impliqués dans la fourniture du service à la sécurité physique et la sécurité de l'information. 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 physique et 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.

d) Le responsable de la sécurité physique du prestataire doit valider formellement le plan de formation concernant la sécurité physique.

7.4. Processus disciplinaire

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

b) Le prestataire doit, sur demande d'un client, lui rendre accessible les sanctions encourues en cas d'infraction aux politiques de sécurité.

7.5. Rupture, terme ou modification du contrat de travail

Le prestataire doit prévoir dans le contrat de travail d'une personne impliquée dans la fourniture du service, lors de la rupture, ou au terme ainsi qu'à la modification de son contrat, les obligations spécifiques de confidentialité.

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 nom des sociétés de maintenance si extérieures ;

- le besoin de sécurité des informations (au sens du paragraphe 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

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 client 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

Il est recommandé (obligatoire pour le Niveau Avancé), 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 paragraphe 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 paragraphe 8.3.

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

9. Contrôle d'accès et gestion des identités

Ce paragraphe 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 client, mais pour lesquels le prestataire met en œuvre les moyens de contrôle d'accès (en fournissant notamment au client une interface de gestion des comptes et des droits d'accès).

Les utilisateurs pour lesquels le client 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 physiques et 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 physique et aux ressources du système d'information du service.

b) Le prestataire doit définir les exigences en matière d'expiration des droits d'accès.

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

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

e) 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 client ainsi que tous les droits d'accès qui leur ont été attribués.

f) Le prestataire doit être en mesure de fournir, pour un utilisateur donné, qu'il soit sous la responsabilité du prestataire ou du client, la liste de tous ses droits d'accès sur les sites et sur les différents éléments du système d'information du service.

g) Le prestataire doit définir une liste des droits d'accès incompatibles entre eux.

h) 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.

i) 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 client 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) ou pouvant avoir un accès physique.

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 paragraphe 10, celles-ci doivent notamment porter sur :

- la gestion des moyens d'authentification (émission et réinitialisation de mots de passe, mise à jour des listes de révocation des certificats (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.

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 en mode SaaS, le prestataire doit proposer à ses clients 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. Des moyens permettant de tracer les accès à ces comptes doivent être implémentés.

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 client.

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

c) Les interfaces d'administration mises à disposition des clients 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 client.

e) Si des interfaces d'administration sont mises à disposition des clients 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 paragraphe 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 clients.

g) Dans le cadre d'un service en mode SaaS, les interfaces d'administration mises à disposition des clients 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 en mode IaaS 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 clients du service en mode IaaS.

j) Lorsque le prestataire utilise un service en mode 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 clients du service en mode PaaS.

9.7. Restriction des accès à l'information

a) Le prestataire doit mettre en œuvre des mesures de cloisonnement informatique et physique appropriées entre ses clients.

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.

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 clients en cas de réallocation d'une ressource ou de récupération du support physique.

- Dans le cas d'un service en mode IaaS, cet objectif pourra par exemple être atteint :
  - par un chiffrement du disque ou du système de fichiers, 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 client.
- Dans le cas d'un service en mode PaaS ou SaaS, cet objectif pourra être atteint en utilisant un chiffrement applicatif dans le périmètre du prestataire, avec au moins une clé par client.
- Dans le cas d'un simple hébergement, cet objectif est du ressort du client.

b) Le prestataire doit utiliser une méthode de chiffrement des données respectant les règles de cryptographie définies dans le document [CRYPTO_B1] annexé à l'arrêté ministériel n° 2018-635 du 2 juillet 2018.

c) 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 paragraphe 11), en fonction du besoin de sécurité des données (voir paragraphe 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 définies dans le document [CRYPTO_B1] annexé à l'arrêté ministériel n° 2018-635 du 2 juillet 2018.

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

c) Si le protocole IPSec est mis en œuvre, le prestataire doit appliquer les recommandations de [NT_IPSEC] de l'ANSSI.

d) Si le protocole SSH est mis en œuvre, le prestataire doit appliquer les recommandations de [NT_SSH] de l'ANSSI.

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 définies dans le document [CRYPTO_B1] annexé à l'arrêté ministériel n° 2018-635 du 2 juillet 2018.

c) 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 définies dans le document [CRYPTO_B1] annexé à l'arrêté ministériel n° 2018-635 du 2 juillet 2018.

10.4. Non répudiation

Lorsque le prestataire met en œuvre un mécanisme de signature électronique, il est recommandé (obligatoire pour le Niveau Avancé) que celui-ci soit conforme au Référentiel Général de Sécurité [RGS] annexé à l'arrêté ministériel n° 2017-835 du 29 décembre 2017.

10.5. Gestion des secrets

a) Le prestataire doit mettre en œuvre des clés cryptographiques respectant les règles définies dans le document [CRYPTO_B2] annexé à l'arrêté ministériel n° 2018-637 du 2 juillet 2018.

b) 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.

c) 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.

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

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

Les zones privées, à accès restreint, 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

Les zones sensibles, à accès nominatif, 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 (obligatoire pour le Niveau Avancé), que le prestataire respecte les recommandations de l'ANSSI publiées sur son site pour mettre en œuvre le 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) 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 sur au moins deux facteurs personnels parmi : la connaissance d'un secret, la détention d'un objet ou la biométrie.

b) Il est recommandé (obligatoire pour le Niveau Avancé), que le prestataire respecte les recommandations de l'ANSSI publiées sur son site 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) Le prestataire doit documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones sensibles.

h) 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.

i) 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 conforme 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

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.

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 (obligatoire pour le Niveau Avancé), 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 privées 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 dès leur parution 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 client y sont stockées chiffrées conformément au paragraphe 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

Le prestataire doit documenter et mettre en œuvre une procédure de transfert hors site de données client, 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

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 client. 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. À noter qu'aucun support ayant détenu des informations classifiées ne peut être recyclé. Il est nécessairement détruit conformément à la réglementation en vigueur.

11.10. Matériel en attente d'utilisation

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

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 lui et pouvant avoir un impact sur la sécurité ou la disponibilité du service, de communiquer au plus tôt à l'ensemble de ses clients 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 en mode PaaS, le prestataire doit informer au plus tôt le client de toute modification à venir sur des éléments logiciels sous sa responsabilité dès lors que la compatibilité complète ne peut être assurée.

d) Dans le cadre d'un service en mode SaaS, le prestataire doit informer au plus tôt le client de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le client.

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

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 paragraphe 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 paragraphes 8 et 11. Les communications entre site principal et site(s) de sauvegarde doivent être protégées par chiffrement, conformément aux exigences du paragraphe 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 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 en accord avec les obligations légales et réglementaires[1].

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

e) Il est recommandé (obligatoire pour le Niveau Avancé), que le système de journalisation mis en place par le prestataire respecte les recommandations de [NT_JOURNAL] de l'ANSSI.

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 paragraphe 3.2 de [NT_JOURNAL] de l'ANSSI.

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 événements 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 paragraphe 8).

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.

[1] Loi n° 1.135, modifiée, Loi n° 1.383, Loi n° 1.430, Loi n° 1.435.

b) Il est recommandé de s'appuyer sur les référentiels d'exigences de détection d'incidents de sécurité, publiés par arrêté ministériel.

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 client, notamment pour leur maintien en condition de sécurité.

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 la PSSI-E et la charte administrateur éditées par l'État. Le prestataire doit mettre en place des mesures de durcissement de la configuration des terminaux utilisés pour les tâches d'administration.

b) 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 paragraphes 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 paragraphe 10.2) ;
- le chiffrement intégral du disque (voir paragraphe 10.1).

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 paragraphe 8.1 a)), 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 ;
- 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 des équipements physiques.

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 clients - avec distinction par client ou ensemble de clients, 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 paragraphe 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 paragraphe 10.2.

d) Le prestataire doit mettre en place et configurer un pare-feu applicatif pour protéger les interfaces d'administration destinées à ses clients 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

Le prestataire doit disposer d'un ou plusieurs dispositifs de détection d'incidents de sécurité sur le système d'information du service. Ces dispositifs 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. Ils doivent être des sources de collecte pour l'infrastructure d'analyse et de corrélation des événements (voir paragraphe 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 paragraphe 12.5).

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

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

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 est conforme à la politique de développement sécurisé du prestataire et permet d'atteindre un niveau de sécurité du développement externe équivalent à celui d'un développement interne (voir exigence du paragraphe 14.1 a)).

14.6. Test de la sécurité et conformité du système

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 des tests utilisés en pré-production.

b) Si le prestataire souhaite utiliser des données client issues de la production pour réaliser des tests, il doit préalablement obtenir l'accord du client 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

Le prestataire doit tenir à jour une liste de l'ensemble 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 être exhaustive, préciser la contribution du tiers au service et tenir compte des cas de sous-traitance à plusieurs niveaux.

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

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 paragraphe 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 clients sans délais conformément au paragraphe 12.2 et mettre en œuvre les mesures permettant de rétablir le niveau de sécurité précédent.

15.5. Engagements de confidentialité

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 clients 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.

16.2. Signalements liés à la sécurité de l'information ou physique

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 clients de signaler tout incident de sécurité, avéré ou suspecté et toute faille de sécurité.

c) Le prestataire doit communiquer sans délai aux clients les incidents de sécurité et les préconisations associées pour en limiter les impacts. Il doit permettre au client 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 ou physique et prise de décision

a) Le prestataire doit apprécier les événements liés à la sécurité de l'information ou physique 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 client.

b) Le prestataire doit utiliser une classification permettant d'identifier clairement les incidents de sécurité touchant des données relatives aux clients, conformément aux résultats de l'appréciation des risques.

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

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

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

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

16.5. Enseignements tirés des incidents liés à la sécurité de l'information ou physique

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

16.6. Recueil de preuves

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 en 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

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 client dans la convention de service.

17.3. Vérification, révision et évaluation de la continuité d'activité

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

17.4. Disponibilité des moyens de traitement de l'information

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 paragraphe 19.1).

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. Dans la Principauté, le prestataire doit respecter au minimum les textes régissant les éléments suivants :

- les données à caractère personnel ;
- le secret professionnel ;
- l'abus de confiance ;
- le secret des correspondances privées ;
- l'atteinte à la vie privée ;
- le secret de sécurité nationale ;
- l'accès à ou le maintien frauduleux dans un système d'information.

b) 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 prévue au paragraphe 8.3b)).

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

d) 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

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.

b) 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 des serveurs et équipements réseau inclus dans le périmètre 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 accès externes au service ;

- si le service bénéficie de développements internes, l'audit de code source portant sur les fonctionnalités de sécurité implémentées.

18.3. Conformité avec les politiques et les normes de sécurité

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.

18.4. Examen de la conformité technique

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 clients du service. Toute modification de la convention de service doit être soumise à l'acceptation du client.

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

- les responsabilités de chacune des parties : prestataire et tiers impliqués dans la fourniture du service, clients, etc. ;

- les éléments explicitement exclus des responsabilités du prestataire ;

- la localisation du service. La localisation du support doit être précisée lorsqu'il est réalisé depuis un État hors l'Union européenne et hors de la Principauté, comme le permet l'exigence prévue au paragraphe 19.2 d).

c) Le prestataire doit proposer une convention de service appliquant le droit de la Principauté. Le droit applicable doit être identifié dans la convention de service.

d) 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.

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

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

g) 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.

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

i) Le prestataire doit indiquer dans la convention de service qu'il ne peut se prévaloir de la propriété des données transmises et générées par le client. Ces données relèvent de la propriété du client.

j) 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 client.

k) 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.

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

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

m) Le prestataire doit préciser dans la convention de service que le client autorise, conformément au présent référentiel (voir exigence prévue au paragraphe 18.2 b)), 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.

n) Le prestataire doit souscrire une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de la prestation.

19.2. Localisation des données

a) Le prestataire doit documenter et communiquer au client la localisation du stockage et du traitement des données.

b) Le prestataire doit stocker et traiter les données du client :

- au sein de l'Union européenne ou de la Principauté dans le cas de la prestation « Niveau Essentiel » ;
- obligatoirement au sein de la Principauté dans le cas d'une prestation « Niveau Avancé » sauf dérogation écrite donnée par le Directeur de l'AMSN. Le prestataire ne devra pas être soumis à des contraintes judiciaires extraterritoriales d'un gouvernement.

c) Les opérations d'administration et de supervision du service doivent être réalisées :

- depuis l'Union européenne ou la Principauté dans le cas de la prestation « Niveau Essentiel » ;
- obligatoirement au sein de la Principauté dans le cas d'une prestation « Niveau Avancé » sauf dérogation écrite donnée par le Directeur de l'AMSN. Le prestataire ne devra pas être soumis à des contraintes judiciaires extraterritoriales d'un gouvernement.

d) Le prestataire peut réaliser des opérations de support aux clients :

- depuis un État hors de l'Union européenne ou de la Principauté dans le cas de la prestation « Niveau Essentiel » ;
- obligatoirement au sein de la Principauté dans le cas de prestation « Niveau Avancé » sauf dérogation écrite donnée par le Directeur de l'AMSN. Le prestataire ne devra pas être soumis à des contraintes judiciaires extraterritoriales d'un gouvernement.

Le prestataire doit documenter la liste des opérations qui peuvent être effectuées par le support client, et les mécanismes permettant d'en assurer le contrôle d'accès et la supervision depuis l'Union européenne ou la Principauté.

19.3. Régionalisation

a) Le prestataire doit s'assurer que les interfaces du service accessibles au client sont 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 client, 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 client. Cet 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 client décrit au paragraphe 10.1 ;
- recyclage sécurisé, dans les conditions énoncées au paragraphe 11.9.

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

Appendice 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[art18]	Arrêté ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié. Disponible sur https://amsn.gouv.mc
[PSSI-E]	Politique des Systèmes d'Information de l'État (PSSI-E), annexée à l'arrêté ministériel n° 2017-56 du 1er février 2017 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée. Disponible sur https://amsn.gouv.mc
[RGS]	Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée. Disponible sur https://amsn.gouv.mc
[PASSI]	Référentiel d'exigences applicables à un Prestataire d'Audit de la Sécurité des Systèmes d'Information : Arrêté ministériel n° 2017-625 du 16 août 2017 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée. Disponible sur https://amsn.gouv.mc

---

II. Normes et documents techniques

Renvoi	Document
[EX_DONNEES]	Documents d'exigences supplémentaires 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 : Arrêté ministériel n° 2018-635 du 2 juillet 2018 portant application de l'arrête ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée. Disponible sur https://amsn.gouv.mc

Renvoi	Document
[CRYPTO_B2]	Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques : Arrêté ministériel n° 2018-637 du 2 juillet 2018 portant application de l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée. Disponible sur https://amsn.gouv.mc
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, AMSN. Disponible sur https://amsn.gouv.mc
[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
[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, note technique n° DAT-NT-22/ANSSI/SDE/NP du 20 février 2015, ANSSI. Disponible sur http://www.ssi.gouv.fr
[NT_MDP]	Recommandations de sécurité relatives aux mots de passe, note technique n° DAT-NT-001/ANSSI/SDE/NP du 5 juin 2012, 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
[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 AMSN, version en vigueur, disponible sur https://amsn.gouv.mc
[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

Appendice 2 Recommandations aux commanditaires

Cet appendice liste les recommandations de l'AMSN aux commanditaires de prestations d'informatique en nuage ou d'hébergement.

a) Le commanditaire peut, lorsqu'il est une autorité administrative ou un opérateur d'importance vitale, demander à l'AMSN 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'AMSN ; la qualification d'un prestataire d'informatique en nuage ou d'hébergement 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, il est recommandé que le commanditaire :

- choisisse le prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'AMSN ;
- exige 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'externalisation de l'AMSN.

e) Le commanditaire peut, conformément au processus de qualification des prestataires de service de confiance, déposer auprès de l'AMSN 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 au sens de l'arrêté ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

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) conformément à l'arrêté ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

imprimé sur papier PEFC

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO