|  |
| --- |
| PLan d’assurance sécurité fournisseur |

|  |  |
| --- | --- |
| DATE | jeudi 30 octobre 2025 |
| DESTINATAIRES | Fournisseurs |
| COPIE | CLOULAS Silvain  VINCENT Christophe  DURQUETY Jean  VAN DEN HEUVEL Thomas |
| EMETTEUR | ROUSVAL Olivier |
| OBJET | Plan d’Assurance Sécurité Fournisseur |

|  |  |
| --- | --- |
| **Classification du document** | **INTERNE** |

# Propriétés du document

## Titre

|  |  |
| --- | --- |
| Titre du document | PAS-F [nom] [nom Société] |

## Documents de référence

|  |  |
| --- | --- |
| Contrat | [N° AO 25-08 DSI/AK - **Tierce Maintenance Applicative** (TMA) du parc applicatif Low Code Outsystems] |

## Suivi des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| Gestion des versions | | | |
| **Version** | **Date** | **Auteur(s)** | **Commentaires** |
| 1 | 02/06/20 | O. ROUSVAL | Création |
| 2 | 04/06/20 | O. ROUSVAL | Quelques ajustements |
| 2.1 | 29/11/21 | O. ROUSVAL | Mise à jour |
| 2.2 | 02/03/22 | O. ROUSVAL | Mise à jour |
| 2.3 | 31/05/2023 | O. ROUSVAL | Mise à jour nouveau DSI |
|  |  |  |  |
|  |  |  |  |

## Destinataires du document – Interne Agence de la Biomédecine

|  |  |
| --- | --- |
| **Entités** | **Noms** |
| DSI | CLOULAS Silvain |
| DSI | VINCENT Christophe |
| DSI | DURQUETY Jean |
| Direction Juridique | VAN DEN HEUVEL Thomas |

**Entre**

« Les parties » telles que définies au Contrat

SOMMAIRE

[1 Propriétés du document 2](#_Toc94702602)

[1.1 Titre 2](#_Toc94702603)

[1.2 Documents de référence 2](#_Toc94702604)

[1.3 Suivi des modifications 2](#_Toc94702605)

[1.4 Destinataires du document – Interne Agence de la Biomédecine 3](#_Toc94702606)

[2 Préambule 6](#_Toc94702607)

[3 Mode opératoire de réponse 7](#_Toc94702608)

[4 Description de la prestation ou du service 8](#_Toc94702609)

[5 Exigences de sécurité 9](#_Toc94702610)

[5.1 Cadre juridique 9](#_Toc94702611)

[5.2 Organisation de la sécurité 14](#_Toc94702612)

[5.3 Audit et contrôles de sécurité 20](#_Toc94702613)

[5.4 Sécurité des environnements 24](#_Toc94702614)

[5.5 Sécurité des données 28](#_Toc94702615)

[5.6 Sécurité des accès logiques 34](#_Toc94702616)

[5.7 Revue et suivi des comptes du domaine de responsabilités du Prestataire 39](#_Toc94702617)

[5.8 Traçabilité des accès logiques 40](#_Toc94702618)

[5.9 Sécurité réseau et télécoms 44](#_Toc94702619)

[5.10 Traçabilité des accès réseau 49](#_Toc94702620)

[5.11 Sécurité physique 51](#_Toc94702621)

[5.12 Plan de continuité de service 58](#_Toc94702622)

[5.13 Sécurité des astreintes 60](#_Toc94702623)

[5.14 Sécurité lors de la réversibilité 61](#_Toc94702624)

[5.15 Engagement sur les accès au système d’information de l’Agence de la Biomédecine 63](#_Toc94702625)

[6 Modification des éléments constitution du PAS-F 64](#_Toc94702626)

[7 Responsabilités et pénalités 65](#_Toc94702627)

[8 APPROBATION 66](#_Toc94702628)

***\*\*\****

# Préambule

En vertu du Contrat, les Parties sont convenues d’adopter le présent document (ci-après « PAS-F »), concernant les prestations de services informatiques, ceci englobe les prestations de type (liste non exhaustive) :

* Software as a Service (SaaS) ;
* Fourniture de service tel que « infrastructure as a service (IaaS) », « platform as a service (PaaS) », recourant en tout ou partie au « cloud computing » ;
* Centre de Services (CdS) ;
* Projet ;
* Etc.

Le présent document vise à formaliser les responsabilités du Prestataire qui intervient dans le cadre du Contrat d’une part, et les exigences de sécurité que le Prestataire s’engage à respecter d’autre part.

L’Agence de la Biomédecine sollicite le Prestataire pour la mise en place d’un partage d’informations unidirectionnel ou bidirectionnel, permettant aux employés habilités du Prestataire de mettre à disposition une prestation ou un service localisé hors du système d’information de l’Agence de la Biomédecine.

Ce document règlemente les conditions d’échanges d’informations dans le cadre du Contrat. Le Prestataire peut disposer d’un accès au Système d’Information de l’Agence de la Biomédecine soit pour y effectuer les activités, soit dans le cadre d’une connexion automatisée de l’objet de la prestation, dans des environnements définis devant être décrits dans le Document d’Architecture Technique (DAT) ou documents équivalent (contrat, documentation technique, etc.).

Il est attendu de la part du Prestataire le respect des exigences de sécurité auxquelles il s’engage (cf. chapitre concernant les exigences de sécurité) et des clauses de sécurité complémentaires du présent document (cf. chapitres correspondants). Les principes sont notamment issus de la norme ISO 27002:2005 et des recommandations de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI).

Ci-dessous les thématiques de sécurité abordées

* Cadre juridique
* Organisation de la sécurité
* Audits et contrôles de sécurité
* Sécurité des environnements
* Sécurité des données
* Sécurité des accès
* Sécurité réseau
* Sécurité physique
* Plan de continuité de service
* Sécurité des astreintes
* Sécurité lors de la réversibilité

# Mode opératoire de réponse

Il est demandé au Prestataire d’être conforme à l’ensemble des exigences applicables du PAS-F au démarrage de la Prestation.

Pour chaque exigence, le Prestataire coche son niveau d’engagement (conforme, non-conforme ou N/A) et décrit explicitement ses engagements dans la rubrique « engagement du Prestataire » :

* Celui-ci a obligation de décrire l’organisation et les moyens opérationnels prévus pour être en conformité vis-à-vis de l'exigence. Les réponses aux exigences doivent être le plus explicite possible ;
* Les éventuelles raisons d’une non-conformité, en fournissant des propositions alternatives/complémentaires pour répondre au plus près de l'exigence ; ces raisons doivent être exceptionnelles car les exigences du présent document relèvent de l’état de l’art en matière de sécurité des Systèmes d’Information. Les éventuelles non-conformités seront soumises à la validation des bénéficiaires de la prestation.
* Si une exigence est « Non Applicable », il sera nécessaire de fournir les raisons liées au contexte de la prestation.

L’Agence de la Biomédecine pourra demander des précisions sur les engagements s’ils considèrent que les réponses apportées par le Prestataire sur la conformité des engagements sont insuffisantes.

Le niveau d’engagement à une exigence, conforme/non conforme ou non applicable est le résultat d’un accord, issu de négociations éventuelles, entre le Prestataire et l’Agence de la Biomédecine.

# Description de la prestation ou du service

*Le Prestataire rappelle ici succinctement (quelques lignes) l’objet du service ou de la Prestation*

# Exigences de sécurité

Le présent paragraphe a pour but de préciser les engagements de sécurité attendus concernant la sécurité informatique et organisationnelle qui encadre la prestation contractée objet du Contrat.

## Cadre juridique

### Loi informatique et liberté

Le Prestataire s’engage à traiter l’ensemble des informations mises à sa disposition dans le cadre de la prestation conformément à la LIL : Respect de la protection des données personnelles (loi n°78-17 du 6 janvier 1978, et ses évolutions).

### Réglementation spécifique

Si, dans le cadre de la prestation contractualisée, une réglementation particulière met en défaut le respect des exigences de sécurité de l’Agence de la Biomédecine, alors le Prestataire doit :

* Informer l’Agence de la Biomédecine de ce changement AVANT sa mise en œuvre effective ;
* Montrer, s’ils existent, les moyens mis en œuvre par le Prestataire pour maintenir le respect des exigences de sécurité de l’Agence de la Biomédecine.

### Respect des contraintes sur les données de santé

|  |  |  |
| --- | --- | --- |
| Si des données de santé sont stockées dans le cadre de la prestation, le Prestataire doit justifier qu’il respecte toutes les exigences légales liées au traitement de données de santé (ex : archivage légal de données). | | |
| **Précisions**:  Si l'objet de la prestation concerne des données de santé alors celles-ci doivent de préférence être hébergées en France dans les conditions définies dans le cadre réglementaire HDS.  Le Prestataire doit justifier qu’il respecte l’ensemble des exigences, liées au traitement des données de santé, établies par les lois et par la doctrine administrative, en particulier concernant l’archivage des données, le respect des formats d’origine, et la durée de conservation. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Niveau de confidentialité ; * Durée de conservation des données ; * Mécanismes d'archivage ; * Mesures de protection associées ; * Etc. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « Non Conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Localisation géographique des services et des données

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, sur le périmètre de la prestation, à spécifier préalablement et précisément les lieux géographiques dans lesquels sont localisés :   * Les données informatiques liées à la prestation ; * Les services objets de la prestation ; * Les personnes participantes à la réalisation de la prestation.   De même, le Prestataire précise si ses infrastructures (techniques ou organisationnelles) sont gérées par une entité juridique appartenant à un pays disposant de lois autorisant l’État à accéder aux données (ex. « PatriotAct » aux Etats-Unis).  Le Prestataire s'engage à ne pas déplacer les données de l’Agence de la Biomédecine sur un autre environnement que ceux définis dans la prestation, sans avoir préalablement reçu une autorisation formelle de l’Agence de la Biomédecine . | | |
| **Précisions** :  Indiquer notamment :   * La liste des lieux géographique d’hébergement des données (et des sites de backup) ; * Les principes de remonter d’information à l’Agence de la Biomédecine en cas de modification en cours de contrat de localisation des lieux d’hébergement des données ou des services. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Pour le Prestataire et ses sous-traitants (tiers éditeur, tiers hébergeur, tiers exploitant, etc.) : * Numéros de SIRET des établissements concernés ; * Procédure de remontée d'information vers l’Agence de la Biomédecine en cas de modification des lieux d'hébergement. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Certifications du Prestataire

|  |  |  |
| --- | --- | --- |
| Si le Prestataire déclare qu’il dispose d’une certification applicable sur le périmètre de la prestation, il s’engage à fournir le justificatif de certification à l’Agence de la Biomédecine. | | |
| **Précisions** :  Préciser les certifications détenues et incluses dans le périmètre de la prestation ainsi que :   * La date du prochain contrôle de certification ; * Le périmètre définis dans le rapport de certification.   Indiquer si les rapports de certifications peuvent être communiqués à l’Agence de la Biomédecine | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Certifications ; * Périmètres certifiés ; * Rapports de certification. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Répercussion des clauses sur les sous-traitants

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, pour l’ensemble des informations manipulées et services mis en œuvre dans le cadre de la prestation, à spécifier précisément à l’Agence de la Biomédecine les opérateurs (sociétés et fournisseurs) amenés à intervenir en cotraitance et sous-traitance.  Le Prestataire doit répercuter les clauses du présent PAS-F dans ses contrats de sous-traitance et de cotraitance et s’assurer de leur mise en œuvre effective.  Le Prestataire s'engage à respecter cette exigence dans le cas où un contrat de sous-traitance viendrait à être signé ultérieurement à la signature du contrat avec l’Agence de la Biomédecine. | | |
| **Précisions** :  Indiquer la liste des sous-traitants amenés à intervenir sur la prestation.  Décrire comment les clauses du présent PAS-F sont appliquées et contrôlées auprès des sous-traitants du prestataire. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Raison sociale des sous-traitants intervenant dans le cadre de la prestation ; * Dispositifs contractuels et opérationnels de répercussion des clauses du présent PAS-F auprès des sous-traitants (contrat, PAS-F, convention, etc.) ; * Procédure de remontée d'information vers l’Agence de la Biomédecine en cas de modification, en cours de contrat, de la liste des sous-traitants. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Organisation de la sécurité

### Responsabilités et rôles sécurité

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit désigner parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment :   * L'interlocuteur privilégié de l’Agence de la Biomédecine pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d’investigations initiées par l’Agence de la Biomédecine ou le Prestataire ; * Suite à des incidents de sécurité opérationnels ; * Chargé du maintien et de la mise en application du PAS-F.   Ce correspondant doit être joignable aux horaires convenus dans le cadre contractuel. Tout remplacement de ce correspondant doit être notifié à l’Agence de la Biomédecine préalablement à son entrée en vigueur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité. | | |
| **Précisions** :  Préciser la fonction de la personne responsable de la mise en œuvre et du respect du PAS (le nom et les coordonnées seront fournis dans l’annuaire de la prestation, ses rôles et missions seront détaillés dans le PQS ou document équivalent).  Un engagement de devoir d’alerte en cas de changement de responsable est également attendu. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Documents présentant le rôle, les responsabilités et les coordonnées du Responsable de la Sécurité de la Prestation (annuaire, PQS et support de sensibilisation). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Pilotage de la SSI

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit aborder les aspects sécurité dans le cadre de la gouvernance de la prestation.  Il décrit, au PQS de la prestation ou tout document équivalent, les points suivants :   * Les instances de pilotage de la prestation dans lesquelles la sécurité pourra être abordée * La fréquence à laquelle la sécurité sera abordée (au minimum trimestrielle) * Les acteurs sécurité du Prestataire et de l’Agence de la Biomédecine y participant   Le PQS, ou document équivalent, doit être validé par l’Agence de la Biomédecine au démarrage de la prestation. | | |
| **Précisions** :  Le PQS, ou document équivalent, doit être validé par l’Agence de la Biomédecine au démarrage de la prestation. | | |
| Exemples de preuves attendues lors des audits et contrôles :   * PQS ou document équivalent validé ; * Validation de la gouvernance sécurité par l’Agence de la Biomédecine (mail, compte-rendu, document version validée). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Détection, alerte et traitement des incidents de sécurité

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit disposer, sur le périmètre de la prestation, d’un processus formalisé et opérationnel de gestion des incidents de sécurité. Celui devra tenir compte des phases suivantes :   * Détection ; * Analyse ; * Traitement ; * Alerte.   Le Prestataire doit permettre à l’Agence de la Biomédecine de participer au traitement de l’incident le cas échéant.  Des réunions périodiques d’analyse post-incident devront être planifiées avec l’Agence de la Biomédecine pour le traitement des causes profondes.  Le processus de gestion des incidents de sécurité doit être revu et approuvé par la DSI de l’Agence de la Biomédecine. | | |
| **Précisions** :  L'incident de sécurité est protéiforme, il peut être défini à partir de   * La typologie de l'évènement qui s'est produit ; * L’objectif de sécurité recherché ; * La conformité d'un environnement dans un contexte donné.   Nous définirons un incident de sécurité des Systèmes d’information par : un évènement potentiel ou avéré, indésirable ou inattendu, impactant la sécurité de l'information.  L'impact sur la sécurité de l'information peut être évalué par rapport aux critères : Confidentialité, Intégrité, Preuve ou Disponibilité. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :  Le processus de gestion des incidents de sécurité. Il doit décrire :   * Les intervenants, rôles, responsabilités et coordonnées ; * Mode opératoire de qualification, alerte, traitement et clôture des incidents de sécurité ; * Matrice de qualification des incidents de sécurité ; * Validation par l’Agence de la Biomédecine (bénéficiaire de la prestation) du processus de gestion des incidents de sécurité (mail, compte-rendu, post mortem, document version validée). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Gestion de crise sécurité

|  |  |  |
| --- | --- | --- |
| Sur le périmètre SI de la prestation sous sa responsabilité, le Prestataire doit disposer d’un plan de gestion de crise formalisé et opérationnel tenant compte des aspects SSI.  Ce plan doit préciser au minimum :   * Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ; * La composition de la cellule de crise : fonctions et responsabilités des membres (Agence de la Biomédecine et Prestataire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ; * Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).   Le plan de gestion de crise doit être revu et approuvé par l’Agence de la Biomédecine. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :  Le plan de gestion de crise. Il doit décrire :   * Les intervenants, rôles, responsabilités et coordonnées ; * Mode opératoire de qualification, alerte, traitement et clôture d'une crise ; * Matrice de qualification d'une crise ; * Moyens utilisés en cas de crise (salle de crise (adresse postale, numéro de salle), moyens de télécommunication, annuaire) ; * Validation par l’Agence de la Biomédecine (bénéficiaire de la prestation) du plan de gestion de gestion de crise (mail, compte-rendu, document version validée) ; * Compte-rendu d'exercice de crise. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Engagement Individuel de Confidentialité (EIC)

|  |  |  |
| --- | --- | --- |
| L’Agence de la Biomédecine se réserve le droit de faire signer un engagement de confidentialité directement par le salarié et intervenant du prestataire ou toute personne intervenant pour son compte. | | |
| **Précisions** :  Préciser qu’un engagement individuel de confidentialité sera signé par chaque collaborateur intervenant dans le cadre de la prestation. Un exemplaire devra être conservé par chacune des parties. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Engagements Individuels de confidentialité signés ; * Document opérationnel de suivi des signatures. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Sensibilisation des intervenants - Exigence non applicable lorsque l’Agence de la Biomédecine accède à des ressources hébergées par le Prestataire (mode as- a service)

|  |  |  |
| --- | --- | --- |
| **Exigence spécifique - Ressources Prestataire**  Sur la base des informations transmises par l’Agence de la Biomédecine, le Prestataire s’engage à ce que chacun des intervenants sous sa responsabilité dans le périmètre de la Prestation respecte les règles de protection du Système d’Information de l’Agence de la Biomédecine.  En complément, le Prestataire veille à ce que ses intervenants respectent les dispositions concernant la sécurité telles que décrites au Contrat et au présent PAS-F. Notamment :   * L'organisation sécurité de la prestation ; * La Charte de l'utilisateur pour l'usage du Système d’Information de l’Agence de la Biomédecine ; * Protection du patrimoine informationnel de l’Agence de la Biomédecine ; * Le respect de la confidentialité tel que défini au contrat ; * Le signalement des incidents de sécurité ou des suspicions d’incidents de sécurité.   Cette sensibilisation doit être réalisée avant la prise de poste du personnel du Prestataire sur le périmètre de la Prestation, puis annuellement ou en cas d'évolution des règles de protection du Système d’Information de l’Agence de la Biomédecine.  L’Agence de la Biomédecine pourra planifier et organiser avec le Prestataire des sessions de sensibilisation aux enjeux métiers. | | |
| **Précisions** :  Le Prestataire organise à sa charge la sensibilisation appropriée pour garantir le respect de ces mesures.  Les règles de protection du Système d’Information de l’Agence de la Biomédecine seront fournies au démarrage de la Prestation par l’Agence de la Biomédecine notamment sous forme de documentation. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure de sensibilisation des intervenants prestataire (et sous-traitants) de la prestation (nom et fonction des personnes en charge de la sensibilisation, formation orale, fréquence des formations (au démarrage de la prestation et rappel annuel), émargement...) ; * Document support de la sensibilisation : Livret d’accueil comprenant les règles de protection du Système d’Information de l’Agence de la Biomédecine édictées dans les documents réalisés par les parties (PQS, plan de crise, etc.) pour la prestation et ceux fournis par l’Agence de la Biomédecine (PAS-F, chartes Système d’Information, etc.) * Document opérationnel de suivi des signatures. * Attestations individuelles de suivi de formation ou feuilles d'émargement. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Audit et contrôles de sécurité

### Autocontrôle de sécurité - Exigence non applicable lorsque l’Agence de la Biomédecine accède à des ressources hébergées par le Prestataire (mode as- a service)

|  |  |  |
| --- | --- | --- |
| **Exigence spécifique - Ressources Prestataire**  Le Prestataire doit effectuer des autocontrôles de conformité aux exigences du présent PAS-F pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.  Il doit fournir et présenter trimestriellement à l’Agence de la Biomédecine le tableau de bord des indicateurs sécurité formalisant le résultat de ces autocontrôles.  Les indicateurs et le table de bord seront définis une fois l’appel d’offre finalisé. | | |
| **Précisions** :  Les modalités de restitution des autocontrôles de conformité sont à définir avec l’Agence de la Biomédecine avant le démarrage de la prestation. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Table de bord sécurité d'autocontrôle trimestriel complété ou résultats de l'autocontrôle. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Contrôle de sécurité

|  |  |  |
| --- | --- | --- |
| Le Prestataire s'engage à autoriser l’Agence de la Biomédecine à réaliser des contrôles de sécurité, de type « scan de vulnérabilité » ou « test d'intrusion informatique » par exemple.  Sont entendus notamment que :   * Le rapport sera fourni à l’Agence de la Biomédecine ; * Le Prestataire s'engage à collaborer de bonne foi avec l’Agence de la Biomédecine ; * Le coût des contrôles est parti intégrante du contrat ainsi que, le coût induit par la participation aux contrôles d’intervenants du Prestataire. | | |
| **Précisions** :  Le Prestataire spécifie ici son accord ainsi que les modalités d'exécution et le délai de prévenance s'ils ne sont pas précisés au contrat. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :  À constater lors des contrôles :   * Participation aux contrôles ; * Fourniture de preuves relatives aux exigences dans les délais fixés par les contrôleurs. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Sécurité des outils et services - Exigence non applicable lorsque le Prestataire accède à des ressources hébergées par l’Agence de la Biomédecine

|  |  |  |
| --- | --- | --- |
| Le Prestataire démontre que les outils et services mis à disposition de l’Agence de la Biomédecine ne sont pas sujets aux 10 principales vulnérabilités de l'OWASP[[1]](#footnote-1). | | |
| **Précisions** :  Le prestataire décrit ici les dispositifs mis en place pour assurer la détection des vulnérabilités de l'OWASP (types scan, audit et tests d’intrusion). | | |
| **Exemples de preuves attendues lors des audits et contrôles**:   * Rapport des contrôles effectués au minimum une fois par an. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Correction des écarts identifiés

|  |  |  |
| --- | --- | --- |
| En cas d’écarts constatés, avec les exigences de sécurité contractuelles, ou en cas de manquement à la sécurité, suite à un audit ou un contrôle, un plan de remédiation devra être formalisé par le Prestataire au plus tard 15 jours après la livraison du rapport.  Le Prestataire devra ensuite régulariser ces écarts ou manquements par l'application du plan de remédiation dans un délai convenu en commun accord par les deux parties. | | |
| **Précisions** : Les retards pourront donner lieu à des pénalités financières. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Plan d'action de mise en conformité des écarts constatés lors des audits ; * Fourniture du plan d'action dans les 15 jours suivant la constatation des écarts (date de remise du plan d'action (mail, etc.)) | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Sécurité des environnements

### Protection contre les programmes malveillants

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, dans le cadre de la prestation, à installer, sur les équipements qui le supportent (postes de travail et serveurs notamment), des systèmes de protection contre les codes malveillants ainsi qu’à :   * Les mettre à jour régulièrement ; * Ne pas les désactiver même à des fins de résolution d’incident. | | |
| **Précisions** :   * Décrire les solutions en place sur les équipements de la prestation ; * Décrire les politiques de gestion de ces solutions (fréquences de mises à jour des bases antivirales, fréquences de scans des ressources, etc.) ; * Formaliser l'engagement sur la non-désactivation des dispositifs de protection en cas d’incident. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Description de la solution antivirus utilisée sur les équipements ; * Inventaire des équipements affectés à la prestation (postes de travail, serveurs, etc.) ; * Captures d’écran de la solution antivirus utilisée sur un échantillon d'équipements ; * Version de la dernière base de signature installée ; * Version du moteur antivirus et de l'agent antiviral ; * Captures d'écran de la console de gestion antivirale (nombre d'agents déployés sur les équipements, statut actif/inactif). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Suivi de la protection contre les programmes malveillants

|  |  |  |
| --- | --- | --- |
| Un suivi périodique (au minimum hebdomadaire) de l’état de mise à jour des systèmes de protection des postes de travail et serveurs du Prestataire contre les programmes malveillants (version, signatures antivirales) doit être effectué et formalisé. | | |
| **Précisions** :  Décrire la procédure de suivi hebdomadaire du bon déploiement des mises à jour antivirale (récupération des signatures antivirales, déploiement, récupération des logs de déploiement des signatures, plan d’action correctif en cas d’échec, etc.). | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politiques antivirales ; * Procédures de suivi de l’état des mises à jour des signatures antivirales et le mode de collecte (fréquence des mises à jour des signatures antivirales et des scans complets, vision du niveau de la mise à jour globale de tous les équipements (postes de travail, serveurs, etc.), personne réalisant le contrôle, journalisation des contrôles, suivi des contrôles réalisés) ; * Suivi des mises à jour antivirales (compte rendu de suivi de déploiement hebdomadaire des mises à jour) ; * Capture d’écran du paramétrage des mises à jour antivirales sur un échantillon d'équipements de la prestation ; * Capture d’écran du paramétrage de la fréquence des scans sur un échantillon d'équipements de la prestation ; * Processus de traitement en cas d'anomalie. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Correctifs de sécurité

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, dans le cadre de la prestation, à maintenir à jour tous les composants logiciels et techniques qui concourent à la délivrance de l’objet de la prestation, dont :   * Tous les logiciels et systèmes d’exploitation installés sur les équipements d’infrastructure ou réseau ; * Tous les logiciels et systèmes d’exploitation périphériques ; * Tous les logiciels de sécurité.   Il s’engage notamment à réaliser une veille technique et à appliquer les correctifs de sécurité adéquats dans des délais adaptés à la prestation. | | |
| **Précisions** :  Décrire le système de déploiement et de surveillance des correctifs de sécurité sur les composants logiciels et technique de la prestation (postes de travail, serveurs, équipements réseaux, logiciels, *firmwares*, librairies, etc.). En précisant pour chaque type de ressource : les systèmes d’exploitation, éditeurs, fréquences de déploiement, etc. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Description du dispositif permettant le déploiement et la surveillance des correctifs de sécurité (Unix / Windows JBOSS, Redhat, …) sur les équipements (collecte, qualification, déploiement des mises à jour des correctifs de sécurité, périodicité des mises à jour, processus de validation d'un correctif, tests de non-régression) ; * Inventaire des équipements affectés à la prestation (postes de travail, serveurs, etc.) ; * Référentiel des correctifs applicables et plan de déploiement ; * Journal des installations des correctifs de sécurité sur un échantillon d'équipements ; * Capture d’écran de la configuration du système de déploiement des correctifs de sécurité. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Suivi de l'application des correctifs de sécurité

|  |  |  |
| --- | --- | --- |
| Un suivi périodique (mensuel) de l’état de mise à jour des correctifs de sécurité des composants logiciels et techniques du Prestataire doit être effectué et formalisé | | |
| **Précisions** :  Décrire la procédure de suivi hebdomadaire du bon déploiement des correctifs de sécurité (récupération des logs de déploiement, plan d’action correctif en cas d’échec, etc). | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politique(s) de déploiement des correctifs de sécurité ; * Procédure de suivi de l’état des mises à jour des correctifs de sécurité des équipements (niveau de mise à jour de l'ensemble du parc informatique, personne en charge des contrôles, journalisation des contrôles, périodicité) ; * Suivi des mises à jour des correctifs de sécurité (compte rendu de suivi de déploiement mensuel des mises à jour) ; * Traces de suivi des mises à jour des correctifs de sécurité sur un échantillon d'équipements de la prestation. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

## Sécurité des données

### Classification des données

|  |  |  |
| --- | --- | --- |
| Le Prestataire ne communique la classification des données utilisées dans le cadre de la Prestation qu’aux seuls intervenants ayant le « besoin d’en connaître ».  Cette communication doit être faite à l’entrée du personnel du Prestataire et à chaque modification du périmètre applicatif.  Le Prestataire demandera à l’Agence de la Biomédecine la classification des données avant le démarrage des services et à chaque modification du périmètre applicatif. | | |
| **Précisions** :  « Personnes ayant le Besoin d’en connaître » : personnes qui auront potentiellement accès aux données de la prestation et qui doivent être conscients de leur éventuelle sensibilité. A contrario, les intervenants du Prestataire n’accédant pas à des données sensibles utilisées dans le cadre de la Prestation ne doivent pas être informés de leur existence.  La classification des données décrit les types de données utilisées dans le cadre de la prestation ainsi que leur niveau de sensibilité (exemple de type de données : données métier de l’Agence de la Biomédecine). Cette classification est fournie par l’Agence de la Biomédecine au Prestataire au démarrage de la prestation. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Trace de réception de la classification des données par l’Agence de la Biomédecine (mail, etc.) : * Liste des personnes autorisées à disposer de la classification des données ; * Trace de diffusion aux seuls intervenants ayant le « besoin d’en connaître » et/ou les attestations individuelles de réception des seuls intervenants ayant le « besoin d’en connaître » de la classification des données. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Gestion des données

|  |  |  |
| --- | --- | --- |
| L’accès, le stockage, le marquage, l’échange et la destruction des documents et données doivent être sécurisés dans le respect de la politique de de classification des données de l’Agence de la Biomédecine. | | |
| **Précisions** :  La politique de de classification des données de l’Agence de la Biomédecine est fourni en document de référence en même temps que le présent PAS-F. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :  Description des moyens de protection des données mis en œuvre pour respecter les règles définies dans politique de de classification des données de l’Agence de la Biomédecine :   * Impression ; * Destruction ; * Stockage ; * Diffusion/reproduction ; * Échange (mail/courrier) ; * Photos des dispositifs. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Cloisonnement des données de l’Agence de la Biomédecine

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, dans le cadre de la prestation, à mettre en œuvre les moyens techniques et organisationnels pour couvrir les besoins de sécurité des données de l’Agence de la Biomédecine, et notamment assurer qu’elles ne sont en aucune façon accessibles ou visibles par :   * Les autres clients du Prestataire ; * Les intervenants du Prestataire qui n'ont pas le besoin d'en connaître.   Si la prestation prévoit l'hébergement d'environnements de production de l’Agence de la Biomédecine, le Prestataire s’engage à mettre en œuvre et à maintenir un cloisonnement vis à vis des autres environnements (développement, recette, bureautique... par exemple). | | |
| **Précisions** :  Décrire :   * Les moyens de cloisonnement prévus pour la protection des données de l’Agence de la Biomédecine ; * Les engagements en termes de non-utilisation des données en dehors des environnements prévus dans le contrat.   Cette exigence couvre les données propriété de l’Agence de la Biomédecine et également celles :   * Hébergées sur des serveurs de fichiers et de messagerie du Prestataire ; * Produits pour l’Agence de la Biomédecine (livrables) | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Schéma d’architecture * Configuration des VLAN * GPO, ACL, etc. * DAT | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Sauvegarde des données

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s'engage à :   * Mettre en place un système de sauvegarde des données conforme aux besoins exprimés par l’Agence de la Biomédecine ; * Réaliser un suivi mensuel de l’exécution de ces sauvegardes ; * Protéger les sauvegardes avec le même niveau de sécurité que celui appliqué aux données en production ; * Maintenir le même niveau de cloisonnement des données sauvegardées de l’Agence de la Biomédecine vis-à-vis des autres données hébergées par le Prestataire. | | |
| **Précisions** :  Décrire les données que le Prestataire sauvegarde, la fréquence ainsi que les moyens de protection et de cloisonnement des sauvegardes.  NB : Le périmètre sauvegardé peut comprendre les serveurs de données partagées, les environnements applicatifs (production, pré-production, recette, développement, base de gestion des mots de passe) et la base de connaissance dédiée aux informations de connexion administrateurs (identifiants + mot de passe) aux différentes ressources (A faire définir par la MOA lors de la qualification du PAS-F). | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politique de sauvegarde ; * Plan de sauvegarde lié à la prestation ; * Procédure de suivi de l’exécution des sauvegardes (fréquence, acteurs, etc.) ; * Trace de suivi de l’exécution des sauvegardes (compte-rendu, etc.) ; * Preuves relatives aux cloisonnements de données. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Restauration des sauvegardes

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s'engage à :   * Réaliser des tests périodiques de restauration des sauvegardes ; * Communiquer les résultats de ces tests à la demande de l’Agence de la Biomédecine.   Le Prestataire précisera la fréquence de ces restaurations, au minimum semestrielles. | | |
| **Précisions** :  Décrire la procédure de tests de restauration (périmètre, fréquence, comptes rendus, plan d’action en cas d’échec, etc.) | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure des tests de restauration de sauvegarde (date de réalisation des tests, périmètre, journalisation) ; * - Trace d’un test de restauration (logs, compte-rendu, PV). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Stockage des sauvegardes

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit mettre en place des dispositifs de protection des sauvegardes contre les altérations (physiques ou logiques).  Ces dispositifs devront respecter les obligations contractuelles et légales liées à la localisation des services et des données ainsi qu'à leur durée de conservation. | | |
| **Précisions** :  Les dispositifs mis en œuvre peuvent être les suivants : stockage des supports magnétiques dans un coffre étanche et ignifuge ; envoi des sauvegardes vers un site de back-up sécurisé ou un prestataire spécialisé, gestion des droits d’accès, chiffrement, traçabilité des accès, etc. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Description des mécanismes de protection apportés aux sauvegardes (chiffrement, stockage, cloisonnement, purge, etc.) ; * -Liste des lieux de hébergeant les sauvegardes. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Sécurité des accès logiques

### Identifiants du Prestataire

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à définir et appliquer une politique de gestion des identifiants.  Il est attendu du Prestataire :   * Que sa politique privilégie l'utilisation d’identifiants individualisés (rattachés à une personne unique) ; * Qu’il soit en mesure d'expliciter comment il est en mesure de relier à tout instant l'usage d'un compte non individualisé avec l'identité d'une personne.   Les comptes administrateur par défaut doivent être renommés.  Les comptes invités doivent être désactivés. | | |
| **Précisions** :  Décrire :   * Les règles de gestion des identifiants ; * Les règles de gestion des identifiants et des comptes génériques. Le cadre d’utilisation de ces comptes (finalités, cas d’usage, etc.). | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politique de gestion des accès logiques ; * Capture d'écran d'un échantillon de comptes utilisés pour la prestation, sur chaque type de ressource. ; * Tous les types de comptes utilisés doivent apparaître (comptes à privilèges, sans privilèges, compte nominatif et générique, etc.) ; * Liste des comptes génériques et leurs contextes d'utilisation (expression du besoin) ; * Impression d’écran montrant que les comptes « invité » et les comptes créés par défaut lors de l’installation des serveurs intervenant dans le cadre de la prestation, sont bien désactivés ou renommés ; * Politique de gestion de revue des comptes prenant en charge la création/modification/suppression des droits d'accès. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Identifiants de l’Agence de la Biomédecine - Exigence non applicable lorsque le Prestataire accède à des ressources hébergées par l’Agence de la Biomédecine

|  |  |  |
| --- | --- | --- |
| **Exigence spécifique au XaaS (Everything as-a-Service)**  Sur le périmètre de la prestation, le Prestataire doit mettre à disposition un système de gestion individualisé des identifiants de l’Agence de la Biomédecine. | | |
| **Précisions** :  Pour répondre à cette exigence, le Prestataire privilégiera les solutions de type synchrone (Fédération d’Identité) exploitant les informations (identifiants / jetons / privilèges) issus de l’annuaire de l’Agence de la Biomédecine.  Dans le cas d’une solution asynchrone (non fédérée) le Prestataire explicite comment sont opérées les identités : création / modification / suppression et qui est le garant de ce processus. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Cahier des Charges (CDC) ou autre document formalisant le besoin en termes d’identification ; * Capture d'écran prouvant la mise en œuvre des besoins en terme de gestion des identifiants de l’Agence de la Biomédecine sur les ressources de la prestation ; * Procédure de la prestation de gestion des identifiants de l’Agence de la Biomédecine (création / suppression / modification). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Authentification du Prestataire en administrateur

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des authentifiants, pour ses accès en administration. Cela se traduit notamment par :   * L’utilisation de mots de passe de longueur minimale, 10 caractères ; * Une politique de renouvellement, au maximum tous les 90 jours ; * L’utilisation de mots de passes contenant les quatre familles de caractères (lettres minuscules, lettres majuscules, chiffres, caractères spéciaux) ; * L’utilisation de systèmes d’authentification à plusieurs facteurs pour les accès distants.   Les sessions (système ou applicatives) doivent être protégées par des mécanismes de verrouillage automatiques en cas d'inactivité prolongée (au maximum après 10 minutes). | | |
| **Précisions** :  Décrier la politique d’accès (mode de connexion, mot de passe appliquée sur le périmètre de la prestation notamment dans le cadre des accès d’administration, etc..).  Préciser les procédures d’accès distant (HNO / HO).  Préciser s’il y a lieu la politique BYOD. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :  Politique d’accès des administrateurs fonctionnels et techniques du prestataire utilisée dans le cadre de la prestation.  Capture d'écran des politiques de mot de passe implémentée (ex GPO sous Windows) sur les serveurs, équipements réseaux et postes de travail (comptes administrateurs) indiquant :   1. La robustesse du mot de passe en termes de longueur et de complexité ou les mécanismes mis en œuvre (authentification forte) ; 2. La durée de vie du mot de passe / la mise en œuvre d’une authentification forte :  * Procédure d'accès distant des administrateurs prestataires à l'infrastructure hébergeant la prestation ; * Capture d’écran du paramétrage des mécanismes de verrouillage automatique en cas d’inactivité ; * Politique FW poste de travail ; * Blocage port USB ; * Compte administrateur poste de travail inopérant pour les utilisateurs ; * Protocole de connexion distante (VPN, SSH, …) ; * Etc. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Authentification des utilisateurs de l’Agence de la Biomédecine et des intervenants du Prestataire

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des authentifiants conforme aux besoins de sécurité de l’Agence de la Biomédecine.  Cela se traduit au minimum par :   * La possibilité d’utiliser des mots de passe de plus de 8 caractères ; * L’utilisation de mots passes contenant au moins trois parmi les quatre familles de caractères (lettres minuscules, lettres majuscules, chiffres, caractères spéciaux) ; * Une politique de renouvellement, au maximum tous les 90 jours.   Si l’Agence de la Biomédecine met à disposition un système d’authentification à plusieurs facteurs, le Prestataire s'engage à les utiliser conformément aux procédures fournies par l’Agence de la Biomédecine.  Les sessions (système ou applicatives) doivent être protégées par des mécanismes de verrouillage automatiques en cas d'inactivité prolongée (au maximum après 15 minutes). | | |
| **Précisions** :  Décrire les authentifiants de l’Agence de la Biomédecine que le Prestataire compte opérer et la politique de l’authentifiant associée. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politique de mot de passe utilisateurs * Capture d'écran des politiques de mot de passe implémentée (ex GPO sous Windows) sur les postes de travail (administrateurs) indiquant :  1. Robustesse du mot de passe en termes de longueur et de complexité suivant trois parmi les quatre familles de caractères disponibles ou mode d’authentification forte mise en œuvre ; 2. La durée de vie du mot de passe si c’est ce mode d’authentifiant qui est utilisé.  * Capture d’écran du paramétrage des mécanismes de verrouillage automatique en cas d’inactivité prolongé sur les ressources de la Prestation | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Gestion des privilèges

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des privilèges conforme aux bonnes pratiques de sécurité, se traduisant notamment par l'attribution des habilitations selon le principe de moindre privilège et du besoin d'en connaître. | | |
| **Précisions** :  Décrire les différentes typologies de profils existantes et les droits associés ainsi que les processus mis en place pour s’assurer que ces privilèges sont bien respectés.  Préciser notamment les droits accordés aux utilisateurs sur leur poste de travail et sur les serveurs (utilisateur standard, utilisateurs avec pouvoirs, admin local.  Principe de moindre privilège : principes selon lequel chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure de gestion des comptes à privilèges ; * Impression d’écran de la liste des comptes à privilèges de la prestation ; * Description des profils des comptes à privilèges utilisés dans le cadre de la prestation ; * - Expression du besoin d’utilisation des comptes à privilèges. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

## Revue et suivi des comptes du domaine de responsabilités du Prestataire

|  |  |  |
| --- | --- | --- |
| Une revue périodique\*[[2]](#footnote-2) des comptes d’accès aux ressources informatiques (serveurs, postes de travail, applications) du Prestataire utilisé dans le cadre de la prestation doit être effectuée et formalisée. | | |
| **Précisions** :  Décrire les procédures de revue sur les ressources du Système d’Information du Prestataire (postes de travail, serveurs, équipements réseaux) : modes opératoires, périodicités, responsabilités, plan d’action en cas d’écart, etc.  La revue d’emploi consiste à vérifier que les comptes présents dans le système correspondent aux profils des intervenants (comptes d’accès, logiciels autorisés, etc.). Il s’agit également de vérifier que les comptes des collaborateurs ayant quittés la prestation sont bien désactivés sur le périmètre de la prestation.  La revue de « besoin » consiste à vérifier que les droits attribués à chaque profil des intervenants correspondent aux besoins pour mener à bien leurs missions. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure opérationnelle de revue des comptes ; * Preuve (PV, mail, compte-rendu) de revue d'emploi et de besoin. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

## Traçabilité des accès logiques

|  |  |  |
| --- | --- | --- |
| Durant l'exécution de la prestation, le Prestataire met en place, sur ses ressources, des traces qui assurent à tout instant l'imputabilité les actions réalisées. Ces traces contiennent notamment (en fonction de la typologie des ressources) :   * L'identifiant de l'accédant ; * Les connexions et déconnexions aux ressources ; * Les accès fructueux et infructueux aux ressources ; * L'origine des connexions ; * Les actions réalisées (modification, suppression...) ; * Les informations d'horodatage.   et ce pendant une durée au minimum d’un an et en accord avec les exigences légales et réglementaires. Ces traces doivent pouvoir être fournies sur demande de l’Agence de la Biomédecine. | | |
| **Précisions** :  Décrire le dispositif de traçabilité des accès aux ressources du SI Prestataire (contenu des logs, sauvegarde des logs, localisation des sauvegardes, durée de conservation, exploitation éventuelle des logs etc.)  Les ressources du Système d’Information Prestataire sont les serveurs et applications utilisés dans le cadre de la prestation Les accédants sont les utilisateurs et les administrateurs du Prestataire | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politique(s) de gestion des traces décrivant les mécanismes de récupération, de conservation, d'accès, de format, de transmission en cas de demande de l’Agence de la Biomédecine de ces enregistrements ; * - Exemple de trace (avec à minima identifiant, date/heure, action(s) réalisée(s) et statut de la connexion) au niveau des ressources de type système et applicatif. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Suivi des mécanismes de traçabilité des accès logiques

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit s'assurer mensuellement du bon fonctionnement des dispositifs de traçabilité :   * Collecte effective des traces ; * Sauvegarde effective de ces traces.   De plus, le Prestataire s'engage à ne pas désactiver les dispositifs de traçabilité mis en place. | | |
| **Précisions** :  A titre d’exemple, le Prestataire pourra mettre en œuvre, pour répondre à cette exigence, un processus de suivi périodique du bon enregistrement des traces ou un dispositif d'alerte en cas de non-enregistrement et le type de plan d'action en cas d'échec. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure de suivi du bon enregistrement des traces sur les ressources systèmes et applicatives ; * Compte-rendu ou autre preuve de suivi opérationnelle du bon enregistrement des traces. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Gestion des accès au SI de l’Agence de la Biomédecine - Exigence non applicable lorsque l’Agence de la Biomédecine accède à des ressources hébergées par le Prestataire (mode as- a service)

|  |  |  |
| --- | --- | --- |
| **Exigence spécifique au PAS - Ressources Prestataire :**  Les demandes liées aux accès des personnels du Prestataire au Système d’Information de l’Agence de la Biomédecine (création, modification, suppression) doivent être centralisées :   * Le prestataire doit tenir à jour un référentiel de son personnel intervenant dans le cadre de la prestation ; * Le Prestataire suivra la procédure d’accès au Système d’Information de l’Agence de la Biomédecine, fournie par l’Agence de la Biomédecine, pour toute demande d’accès ou de modification de droits ; * Tout personnel du Prestataire qui ne figure pas sur le référentiel ne disposera pas d'un compte d'accès au Système d’Information ; * Les comptes (identifiants et authentifiants) fournis par l’Agence de la Biomédecine sont des comptes nominatifs non transférables à un tiers, même s’il s’agit d’un collaborateur du Prestataire ; * L'arrivée et le départ (et la modification de droits) de personnel du Prestataire doit être notifié à l’Agence de la Biomédecine au fil de l’eau.   Le Prestataire s'assurera auprès de l’Agence de la Biomédecine de la réalisation de revues périodiques\*[[3]](#footnote-3) des comptes d’accès aux ressources informatiques (serveurs, postes de travail, applications) de l’Agence de la Biomédecine utilisées dans le cadre de la prestation. | | |
| **Précisions**:  Indiquer votre engagement de participer aux revues périodiques de comptes du Système d’Information de l’Agence de la Biomédecine attribués aux intervenant Prestataire telles que définies dans l’exigence (postes de travail, serveurs, etc.).  Il s'agit ici des revues de comptes sur le Système d’Information de l’Agence de la Biomédecine.  Les revues seront tracées dans une annexe du présent document : « Personnel Prestataire ».  La revue d’emploi consiste à vérifier que les comptes présents dans le système correspondent aux profils des intervenants (comptes d’accès, logiciels autorisés, etc.). Il s’agit également de vérifier que les comptes des collaborateurs ayant quittés la prestation sont bien désactivés sur le périmètre de la prestation.  La revue de « besoin » consiste à vérifier que les droits attribués à chaque profil des intervenants correspondent aux besoins pour mener à bien leurs missions. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure d’accès au SI de l’Agence de la Biomédecine (interlocuteurs, workflow de demande et validation, modifications de poste ou départs des collaborateurs, etc.) * Preuve (PV, mail, compte-rendu) de revue d'emploi et de besoin * Annexe PAS-F : « Personnel Prestataire » à jour. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Sécurité réseau et télécoms

### Politique de gestion des flux réseau

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des flux réseau, afin de n’autoriser que les flux légitimes.  Par défaut, tous les flux qui ne sont pas explicitement autorisés doivent être interdits. | | |
| **Précisions** :  Décrire les règles de filtrage des équipements réseaux. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Politique ou processus de gestion des flux réseau (ouverture, modification, fermeture, etc.) ; * - Capture d’écran, au niveau des firewall, de la règle de filtrage : « tout ce qui n’est pas explicitement autorisé est interdit ». | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Cartographie des flux

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation le prestataire s’engage à :   * Fournir une matrice exhaustive et à jour des flux mis en œuvre au démarrage de la Prestation ; * Maintenir à jour cette matrice des flux et informer l’Agence de la Biomédecine de toute évolution ; * Effectuer une revue semestrielle de cette matrice. | | |
| **Précisions** :  Décrire le processus de gestion des matrices de flux (définition, maintien, revue). | | |
| Exemples de preuves attendues lors des audits et contrôles :   * Processus de gestion des matrices de flux ; * Matrice des flux techniques avec cartouche des modifications (gestion des versions) ; * Compte rendu de la dernière revue de la matrice de flux ; * DAT. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| Description : | | |

### Interconnexion au SI de l’Agence de la Biomédecine

|  |  |  |
| --- | --- | --- |
| Si la prestation requière une interconnexion entre le réseau de l’Agence de la Biomédecine et le réseau informatique du Prestataire, alors, celui-ci s’engage à proposer une architecture conforme aux prérequis Sécurité des Systèmes d’Information de l’Agence de la Biomédecine. Celle-ci décrira les outils, les équipements, la matrice des flux, les protocoles utilisés.  Cette architecture devra faire l’objet d’une vérification sur le plan sécurité par l’Agence de la Biomédecine.  En cas de modification de l’architecture, celle-ci devra faire l’objet d’une nouvelle vérification par l’Agence de la Biomédecine.  Le Prestataire devra mettre en place les moyens nécessaires pour prévenir un rebond non autorisé depuis son Système d’Information vers le Système d’Information de l’Agence de la Biomédecine (cela peut se traduire par exemple par : un LAN dédié, un serveur d’accès sécurisé…). | | |
| **Précisions** :  Décrire l’architecture et les moyens retenus pour le cloisonnement de son Système d’Information pour éviter tout rebond sur le Système d’Information de l’Agence de la Biomédecine (VLAN, équipements dédiés, etc.).  En complément de cet engagement, fournir le DAT de la prestation. Un résumé du DAT présentant le schéma d’architecture sera annexé au PAS-F.  L’architecture d'interconnexion doit être validée par l’Agence de la Biomédecine. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Schéma d’architecture de la prestation (interconnexion, serveurs hébergeant des données de l’Agence de la Biomédecine, serveurs d’infrastructures, équipements réseaux, postes de travail, connexion nomade, astreintes, protocoles des flux réseaux, systèmes d’exploitation utilisées sur les équipements, représentation des sites et adresses de ceux-ci, etc.). * Preuve de validation de l’architecture de la prestation par l’Agence de la Biomédecine ; * Éventuels schémas d’architecture de la prestation en mode dégradé en explicitant les scénarios de risque ; * - DAT. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Chiffrement des flux

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, dans le cadre de la Prestation, à mettre en place et à maintenir les moyens techniques utiles au chiffrement de tous les flux qui le nécessitent, dont au minimum :   * Tous les flux d’authentification des utilisateurs et des administrateurs ; * Tous les flux relatifs à des accès distants ; * Tous les flux spécifiquement mentionnés au contrat. | | |
| **Précisions** :  Décrire les moyens de chiffrement de flux prévus sur le périmètre de la Prestation. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Matrice des flux techniques ; * Capture d'écran de la configuration des flux d'authentification, des flux relatifs aux accès distants et des flux spécifiques à la prestation (ex : https, VPN, SSH) ; * - DAT. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Prévention contre les attaques externes

|  |  |  |
| --- | --- | --- |
| Le Prestataire mettra en œuvre des dispositifs afin de prévenir les attaques informatiques (intrusions, dénis de service, brute force…) sur le SI utilisé dans le cadre de la prestation. | | |
| **Précisions** :  Décrire les moyens techniques et organisationnels mis en place afin de protéger le service objet de la prestation contre les intrusions (sondes IPS/IDS, proxy, firewall applicatif, etc.) | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * DAT ou équivalent décrivant les dispositifs de protection ; * Enregistrements d'accès non autorisés capturés par les sondes IPS/IDS et/ou firewall(s) ; * Traitements SIEM/SOC. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Traçabilité des accès réseau

|  |  |  |
| --- | --- | --- |
| Les équipements réseau du Prestataire, dans le cadre de la prestation, doivent enregistrer et protéger les traces d’accès au réseau / service, dont au minimum :   * L'adresse IP de l’émetteur ; * L'adresse IP du destinataire ; * La date ; * L'heure.   et ce pendant 1 an ou en accord avec les exigences légales et réglementaires en vigueur.  Ces traces doivent pouvoir être fournies sur demande de l’Agence de la Biomédecine. | | |
| **Précisions** :  Décrire le dispositif d’enregistrement des traces des équipements réseaux (fréquence d’enregistrement, détails des informations enregistrées, délai de rétention, etc.) | | |
| Exemples de preuves attendues lors des audits et contrôles :   * Politique de gestion des traces spécifiant la durée de conservation et les méthodes de conservation de ces traces (lieu de stockage, duplication, accès, etc.) ; * Capture d'écran indiquant l'activation des paramètres d'audit sur les équipements réseaux ; * Exemple de trace réseau d’une transaction sur le périmètre de la prestation. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Suivi des mécanismes de traçabilité des accès réseau

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit s'assurer mensuellement du bon fonctionnement des dispositifs de traçabilité :   * Collecte effective ; * Sauvegarde effective des traces. | | |
| **Précisions** :  A titre d’exemple, le Prestataire pourra mettre en œuvre pour répondre à cette exigence, un processus de suivi périodique du bon enregistrement des traces ou un dispositif d'alerte en cas de non-enregistrement et le type de plan d'action en cas d'échec. | | |
| Exemples de preuves attendues lors des audits et contrôles :   * Procédure de suivi du bon enregistrement des traces sur les ressources réseau ; * Compte-rendu ou autre preuve de suivi opérationnelle du bon enregistrement des traces. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Sécurité physique

### Contrôle des accès physiques aux locaux du prestataire

|  |  |  |
| --- | --- | --- |
| Les locaux du Prestataire, hébergeant les intervenants dans le cadre de la prestation, doivent être équipés d’un dispositif de contrôle d’accès individuel. Toute tentative d’accès à ces locaux doit faire l’objet d’une trace qui doit être conservés au minimum 2 mois.  Le Prestataire restreint ces accès physiques aux stricts besoins opérationnels.  Une procédure de gestion des accès physiques aux locaux du Prestataire doit être formalisée.  Celle-ci doit préciser au minimum les modalités de gestion des demandes et suppressions d’accès ainsi qu'une revue trimestrielle. | | |
| **Précisions** :  Décrire le dispositif de contrôle d’accès physique individuel des bâtiments et plateaux où seront localisés les collaborateurs de la prestation (dispositif d’identification, sas d’accès, traçabilité). | | |
| Exemples de preuves attendues lors des audits et contrôles :   * Procédure de gestion des accès physiques au bâtiment ; * Documentation du dispositif de contrôle d’accès individuel aux bâtiments ; * Photos du dispositif de contrôle d’accès physique ; * Description de la solution/outil de GTB (Gestion technique de Bâtiment) ; * Extraction des traces d’accès aux locaux hébergeant les intervenants dans le cadre de la prestation. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Contrôle des accès physiques aux ressources techniques du Prestataire

|  |  |  |
| --- | --- | --- |
| Les locaux qui hébergent les ressources techniques du Prestataire doivent être équipés d’un dispositif de contrôle d’accès individuel. Toute tentative d’accès à ces locaux doit faire l’objet d’une trace qui doit être conservée au minimum 2 mois.  Le Prestataire restreint ces accès physiques aux stricts besoins opérationnels.  Une procédure de gestion des accès physiques aux locaux techniques du Prestataire doit être formalisée. Celle-ci doit préciser au minimum les modalités de gestion des demandes et suppressions des accès ainsi qu'une revue trimestrielle. | | |
| **Précisions** :  Décrire le dispositif de contrôle d’accès physique individuel des locaux techniques hébergeant les serveurs de données, d’infrastructure et de l’équipement réseau / télécoms (dispositif d’identification, sas d’accès, traçabilité). | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Procédure de gestion des accès physiques aux locaux techniques ; * Documentation du dispositif de contrôle d’accès individuel aux locaux techniques ; * Photos du dispositif de contrôle d’accès physique mis en place au niveau du local technique ; * Extraction des traces d’accès aux locaux hébergeant les ressources techniques du Prestataire. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Protection contre les intrusions physiques dans les locaux hébergeant les ressources techniques du Prestataire

|  |  |  |
| --- | --- | --- |
| Les locaux du Prestataire qui hébergent ses ressources techniques doivent être équipés de dispositifs de détection d’intrusion reliés 24h/24 à un système de surveillance centralisé.  Les traces des évènements, des alarmes, des actions de traitement et de clôture doivent pouvoir être fournies sur demande de l’Agence de la Biomédecine. | | |
| **Précisions** :  Décrire le système de protection contre les intrusions physiques (vidéosurveillance, détecteurs anti-intrusion, société de gardiennage, etc.) prévu pour les locaux techniques hébergeant les serveurs de données, d’infrastructure et de l’équipement réseau. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * **Détecteur :**   + Description des équipements anti-intrusion qui équipent le local technique. Types de détecteurs (volumétrique, infrarouge, etc.) ;   + Photo d’un détecteur d’intrusion protégeant le local technique ;   + Photo de la main courante vérification périodique de fonctionnement du dispositif. * **Alarme :**   + Description du système d’alarme permettant de gérer les alertes d’intrusion ;   + Photo de la centrale d’alarme ;   + Description de l’organisation des interventions en cas d'intrusion | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Certification des sites d'hébergement des ressources techniques

|  |  |  |
| --- | --- | --- |
| Le prestataire indiquera le niveau de certification de ses sites hébergeant les ressources techniques ou le service liés à la prestation.  En l’absence de certification des locaux hébergeant les ressources informatiques ou le service, le Prestataire décrira les systèmes de protection et de surveillance en place contre les évènements pouvant perturber l’activité : incendie, fuite d’eau, fuite de climatisation, défaillance électrique.  Les traces des évènements, des alarmes, des actions de traitement et de clôture doivent pouvoir être fournies sur demande de l’Agence de la Biomédecine. | | |
| Exemples de preuves attendues lors des audits et contrôles :   * Certificats des sites hébergeant les données ou le service ; * Documents décrivant les dispositifs de protection et de surveillance incendie (détection, extinction et centrale de surveillance, modalités d’intervention) ; * Documents décrivant les dispositifs techniques de protection et de surveillance des fuites d’eau et de climatisation (détection, centrale de surveillance, modalités d’intervention) ; * Documents décrivant les dispositifs techniques de protection et de surveillance de défaillance électrique (détection, système de secours, centrale de surveillance, modalités d’intervention). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Protection contre les évènements environnementaux

|  |  |  |
| --- | --- | --- |
| Le Prestataire décrira les risques environnementaux dont font l’objet les sites hébergeant les données ou du service.  En cas de risque avéré, le prestataire précisera les mesures mises en œuvre pour couvrir ces risques (plan de prévention des risques). | | |
| **Précisions** : Préciser notamment les informations relatives aux risques d'inondation | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Plan de prévention des risques ou équivalent ; * Description des solutions de protection associées.   Politique de sécurité physique décrivant les différents moyens de protection mis en œuvre contre les évènements environnementaux extérieurs (inondation, tonnerre, incendie, panne électrique). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Plan de maintenance

|  |  |  |
| --- | --- | --- |
| Un plan de maintenance des infrastructures (bâtiments, énergie, matériels informatiques, télécommunications, etc.) du Prestataire mises en œuvre dans le cadre de la prestation doit être défini et appliqué. | | |
| **Précisions** :  Décrire le Plan de maintenance des infrastructures utilisées sur le périmètre de la prestation (sous-traitants éventuels, risques identifiés et couverts. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Plan de maintenance des infrastructures (personne en charge de la maintenance, société tierce intervenant dans le cadre de la maintenance) ; * Exemple de contrat ou d’intervention de maintenance. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Protection contre le vol - - Exigence non applicable lorsque l’Agence de la Biomédecine accède à des ressources hébergées par le Prestataire (mode as- a service)

|  |  |  |
| --- | --- | --- |
| **Exigence spécifique au PAS-F - Ressources Prestataire :**  Le Prestataire doit mettre en place de mécanismes de protection pour prévenir les vols de terminaux mobiles utilisés dans le cadre de la prestation et réduire leurs impacts. | | |
| Précisions :  Par terminaux mobiles sont entendus : poste de travail, ordinateur portables, tablettes, téléphones.  Le Prestataire s'engage notamment à mettre en place des câbles antivol sur les postes de travail de façon systématique. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Description et photos des dispositifs de protection des postes de travail (câble antivol, etc.) * Description des dispositifs de réduction des impacts en cas de vol de terminaux mobiles (destruction des données à distance, chiffrement, géo localisation, etc.) | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Plan de continuité de service

### Plan de Continuité de Service (PCS)

|  |  |  |
| --- | --- | --- |
| Un plan de continuité de service doit être défini, formalisé en conformité avec les besoins de l’Agence de la Biomédecine . Celui-ci doit préciser au minimum :   * Le périmètre du Prestataire couvert ; * Le niveau de continuité de service fournis (par exemple : DIMA[[4]](#footnote-4), PDMA[[5]](#footnote-5), ...) ; * Les scénarios de sinistre pris en compte ; * Les solutions de secours mises en œuvre ; * Les procédures opérationnelles de secours associées. | | |
| **Précisions** :  Les scénarios attendus, s'ils sont applicables, peuvent notamment être :   * Indisponibilité partielle ou totale des personnels du Prestataire intervenant dans le cadre de la prestation ; * Indisponibilité partielle ou totale des locaux du Prestataire hébergeant du personnel du Prestataire intervenant dans le cadre de la prestation ; * Indisponibilité des infrastructures du Système d’Information du Prestataire utilisées dans le cadre de la prestation. | | |
| **Exemples de preuves attendues lors des audits et contrôles** :  Le PCS avec :   * Description des scénarios de sinistre pris en compte, les délais de reprise identifiés, solutions de secours mises en place pour répondre aux scénarios de sinistre, le processus d’activation) ; * Indication des exigences de continuité définies dans le contrat (SLA, etc.) ; * Exemple de procédures opérationnelles associées. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

### Test du plan de continuité de service

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit tester et mettre à jour son plan de continuité de service au minimum une fois par an. Les résultats de ces tests et exercices seront formalisés et présentés à l’Agence de la Biomédecine. | | |
| **Précisions** :  Indiquer votre engagement sur la réalisation de tests annuels du plan de continuité de service et l’organisation prévue pour la prestation (périodicité, responsabilités, périmètres, durées, etc.). | | |
| **Exemples de preuves attendues lors des audits et contrôles** :   * Plan de tests et d’exercices du PCS (périodicité de réalisation des tests et exercices, plan de réalisation des exercices, journalisation des exercices et tests) ; * Planning de réalisation des exercices et tests du PCS ; * Compte rendu d’exercice ou de test du PCS. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Sécurité des astreintes

### Sécurité des astreintes

|  |  |  |
| --- | --- | --- |
| Dans le cas où des astreintes sont prévues, le Prestataire s'assure qu'il :   * Décrit l'architecture et moyens techniques associés en accord avec l’Agence de la Biomédecine. En cas d'interconnexion au Système d’Information de l’Agence de la Biomédecine, cette architecture et ses évolutions sont soumises à l'exigence : « Validation de l'architecture d'interconnexion » ; * Définit les modalités et procédures d'astreinte en accord avec l’Agence de la Biomédecine (main courante des interventions, déclenchement, attribution de compte d'accès, clôture...) ; * Réalise ses astreintes en accord avec les modalités et procédures définies ; * Maintient le niveau de sécurité exigé par le présent PAS-F. | | |
| **Précisions** :  Décrire la procédure d’accès distant, si ce besoin est prévu dans la prestation. Sinon confirmer l’engagement de respect des règles citées dans l’exigence :   * Tout accès externe éventuel au SI de la prestation depuis un site non prévu contractuellement sera encadré, procéduré et soumis à l’accord de l’Agence de la Biomédecine ; * Toute modification de l’architecture de la prestation doit être soumise à la validation de l’Agence de la Biomédecine. | | |
| **Exemples de preuves attendues lors des audits et contrôles** ;   * Schéma d’architecture de la prestation ; * Procédure d’astreinte ; * Main courante de réalisation d’une astreinte ; * Validation de la procédure par l’Agence de la Biomédecine. | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Sécurité lors de la réversibilité

### Maintien de la sécurité durant la réversibilité ou transfert de la prestation

En cas d'arrêt de la prestation (fin de contrat ou activation de la clause de réversibilité par exemple), pendant toute la durée de la phase de transfert associée, le Prestataire doit assurer le maintien du niveau de sécurité de la prestation décrit dans les documents contractuels.

Pour le respect de certaines exigences légales, les exigences du présent PAS-F liées à la conservation des traces sont toujours applicables après l’arrêt de la prestation.

### Destruction des données en fin de prestation

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit disposer d’une procédure permettant la restitution et la destruction définitive des données de l’Agence de la Biomédecine.  Cette procédure décrit notamment :   * La destruction des données présentes sur tous les environnements (production, préproduction, qualification, développement…) ; * La destruction des données présentes sur des supports de sauvegardes, même si ceux-ci sont mutualisés.   Le Prestataire doit informer l’Agence de la Biomédecine sur le délai de destruction effective de ces données.  Le Prestataire doit fournir un rapport de destruction qui mentionne au minimum :   * Le succès ou l’échec de l’opération ; * Les algorithmes ou la méthode utilisée pour la destruction.   Cette exigence court jusqu’à la destruction effective des données (exemple : logs, données de santé, …). | | |
| **Précisions** :  Décrire la procédure de transfert et de destruction utilisée dans sur le périmètre de la prestation.  Préciser la clause contractuelle liée à cette exigence s’il y a lieu. | | |
| Exemples de preuves attendues lors des audits et contrôles :   * Processus de restitution des données ; * Procédure décrivant les mécanismes permettant la restitution et la destruction définitive des données ; * Description des moyens de destruction des données ; * PV de destruction des données (modèle ou document complété si une destruction a déjà eu lieu). | | |
| **Engagement Prestataire :** | | |
| Noté « Conforme » | Noté « non conforme » | Noté « Non Applicable » |
| **Description** : | | |

## Engagement sur les accès au système d’information de l’Agence de la Biomédecine

### Modifications, restrictions et interruption d’accès

Il est indiqué qu’en cas d’impératif qui nécessite d’intervenir sans délai sous peine de compromettre la sécurité ou le bon fonctionnement du Système d’Information et après en avoir averti le Prestataire dans la mesure de ses possibilités, l’Agence de la Biomédecine peut modifier, restreindre ou interrompre à tout moment tout ou partie des accès à son Système d’Information de l’objet du Contrat ce qui aurait pour conséquence pour l’Agence de la Biomédecine ou le Prestataire une impossibilité d’assurer tout ou partie des prestations ou services demandés.

L’Agence de la Biomédecine en avisera le Prestataire dans les meilleurs délais.

L’Agence de la Biomédecine pourra également procéder à toutes les modifications, restrictions ou suspensions des accès à son Système d’Information dans tous les cas où le Prestataire ou les personnes dont il doit répondre ne se conformeraient pas aux obligations de sécurité telles que décrites dans le présent document.

Dans le cas où les modifications, les restrictions ou les interruptions sont liées à un cas de force majeure, les dispositions correspondantes des articles du Contrat s’appliqueront.

Si la suppression des accès devait durer plus de trois (3) jours, les Parties se rencontreraient dans les conditions définies dans le Contrat.

# Modification des éléments constitution du PAS-F

Des modifications peuvent être apportées au PAS-F, sous forme d’avenants, dans les cas d’évolutions significatives.

Par exemple et de manière non limitative :

* Suite à une évolution de l’analyse des risques sur le périmètre de la prestation ;
* Suite à une modification des modalités d'accès à l’objet de la prestation ;
* Modification de la souscription au service objet de la prestation ou modification du Contrat ;
* Modification de l’architecture technique du Prestataire impactant l’objet de la prestation, dont, le changement de localisation des données, la modification des fonctionnalités de l’objet de la prestation.

Suite à une mise à jour qui impact les modalités de la prestation.

La prise en compte des modifications dans le PAS-F est effectuée par l’Agence de la Biomédecine.

L’application d’éventuelles nouvelles exigences de sécurité prend effet dès la signature par les deux Parties d’un avenant au présent PAS-F.

Toute modification du présent document ne sera acceptée que si elle fait l’objet d’un accord écrit et signé par les représentants autorisés des deux Parties.

# Responsabilités et pénalités

Toute modification unilatérale des présentes dispositions engage la responsabilité de la Partie qui en est à l’origine, à l’égard de l’autre Partie.

En cas de non-respect du PAS-F, le titulaire sera redevable du paiement de pénalités. Les modalités de calcul et d’application des pénalités sont précisées au Contrat.

# APPROBATION

Etabli en deux exemplaires originaux à \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ le

|  |  |
| --- | --- |
| Pour l’Agence de la Biomédecine [fonction]  [Nom, prénom] | Pour le prestataire, [fonction]  [Nom, Prénom] |
|  |  |

(Signatures précédées de la mention manuscrite « Lu et Approuvé » avec paraphes des représentants des Parties sur chacune des pages du présent document).

1. https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_Top\_10.html [↑](#footnote-ref-1)
2. Une revue « d’emploi » (au minimum trimestrielle), une revue de « besoin » (au minimum annuelle). [↑](#footnote-ref-2)
3. Une revue « d’emploi » (au minimum trimestrielle), une revue de « besoin » (au minimum annuelle). [↑](#footnote-ref-3)
4. *Durée Interruption Maximal Admissible* [↑](#footnote-ref-4)
5. *Perte de Données Maximale Admissible* [↑](#footnote-ref-5)