|  |
| --- |
|  |
| annexe 2 - Précisions pacs groupe sncf |

L’annexe Précisions PACS Groupe SNCF est un document apportant des précisions au Plan d’Assurance Cybersécurité de la Prestation.

Il a pour objectifs de :

* Fournir des précisions sur les exigences de sécurité ;
* Indiquer des exemples de preuves sur les exigences de sécurité.

SOMMAIRE

[1. Exigences de sécurité 4](#_Toc165297862)

[1.1. Cadre juridique - JUR 4](#_Toc165297863)

[JUR 01 : Réglementation spécifique 4](#_Toc165297864)

[JUR 02 : Localisation géographique des services et des données 4](#_Toc165297865)

[JUR 03 : Certifications du Prestataire 4](#_Toc165297866)

[JUR 04 : Répercussion des clauses sur les sous-traitants 4](#_Toc165297867)

[1.2. Organisation de la sécurité – ORG 5](#_Toc165297868)

[ORG 01 : Responsabilités et rôles sécurité 5](#_Toc165297869)

[ORG 02 : Pilotage de la SSI 5](#_Toc165297870)

[ORG 03 : Détection, alerte et traitement des incidents de sécurité 6](#_Toc165297871)

[ORG 05 : Gestion de crise sécurité 6](#_Toc165297872)

[ORG 06 : Engagement Individuel de Confidentialité (EIC) 6](#_Toc165297873)

[ORG 07 : Sensibilisation des intervenants à la sécurité informatique 7](#_Toc165297874)

[ORG 08 : Sensibilisation des intervenants au SI SNCF 7](#_Toc165297875)

[ORG 09 : Identification de suppléants des personnels clés 7](#_Toc165297876)

[1.3. Audit et Contrôles de sécurité - CTRL 8](#_Toc165297877)

[CTRL 01 : Autocontrôle de sécurité 8](#_Toc165297878)

[CTRL 02 : Contrôles de sécurité du SI 8](#_Toc165297879)

[CTRL 03 : Auditabilité du PACS 8](#_Toc165297880)

[CTRL 04 : Sécurité des outils et services 8](#_Toc165297881)

[CTRL 05 : Contrôle des connexions d’administration distantes 9](#_Toc165297882)

[CTRL 06 : Correction des écarts identifiés 9](#_Toc165297883)

[1.4. Sécurité des environnements - ENV 9](#_Toc165297884)

[ENV 02 : Protection contre les programmes malveillants 9](#_Toc165297885)

[ENV 03 : Suivi de la protection contre les programmes malveillants 9](#_Toc165297886)

[ENV 04 : Maintien en condition de sécurité 10](#_Toc165297887)

[ENV 05 : Suivi de l'application des correctifs de sécurité 10](#_Toc165297888)

[1.5. Sécurité des données - DATA 10](#_Toc165297889)

[DATA 01 : Classification des données 10](#_Toc165297890)

[DATA 02 : Gestion des données 11](#_Toc165297891)

[DATA 03 : Cloisonnement des données du Client 11](#_Toc165297892)

[DATA 04 : Sauvegarde des données 11](#_Toc165297893)

[DATA 05 : Restauration des sauvegardes 12](#_Toc165297894)

[DATA 06 : Stockage des sauvegardes 12](#_Toc165297895)

[1.6. Sécurité des accès logiques - SAL 12](#_Toc165297896)

[SAL 01 : Identifiants du Prestataire 12](#_Toc165297897)

[SAL 02 : Identifiants du Client sur le SI Prestataire 12](#_Toc165297898)

[SAL 03 : Authentification du Prestataire en administration 13](#_Toc165297899)

[SAL 04 : Existence d’un bastion pour se connecter en administration 13](#_Toc165297900)

[SAL 05 : Gestion des privilèges 13](#_Toc165297901)

[SAL 06 : Revue et suivi des comptes du domaine de responsabilités du Prestataire 13](#_Toc165297902)

[SAL 07 : Traçabilité des accès logiques 14](#_Toc165297903)

[SAL 08 : Suivi des mécanismes de traçabilité des accès logiques 14](#_Toc165297904)

[SAL 09 : Suivi du personnel du prestataire 14](#_Toc165297905)

[1.7. Sécurité réseau - RES 15](#_Toc165297906)

[RES 01 : Politique de gestion des flux réseau 15](#_Toc165297907)

[RES 02 : Cartographie des flux 15](#_Toc165297908)

[RES 03 : Interconnexion au SI du Client 15](#_Toc165297909)

[RES 05 : Chiffrement des flux 15](#_Toc165297910)

[RES 06 : Prévention contre les attaques externes 15](#_Toc165297911)

[RES 07 : Traçabilité des accès réseau 16](#_Toc165297912)

[RES 08 : Suivi des mécanismes de traçabilité des accès réseau 16](#_Toc165297913)

[1.8. Sécurité physique - PHYS 16](#_Toc165297914)

[PHYS 01 : Contrôle des accès physiques aux locaux du Prestataire 16](#_Toc165297915)

[PHYS 04 : Contrôle des accès physiques aux ressources techniques du Prestataire 16](#_Toc165297916)

[PHYS 05 : Protection contre les intrusions physiques dans les locaux hébergeant les ressources techniques du Prestataire 17](#_Toc165297917)

[PHYS 06 : Certification des sites d'hébergement des ressources techniques 17](#_Toc165297918)

[PHYS 07 : Protection contre les évènements environnementaux 17](#_Toc165297919)

[PHYS 08 : Plan de maintenance 17](#_Toc165297920)

[PHYS 09 : Protection contre le vol du matériel 17](#_Toc165297921)

[PHYS 10 : Sécurisation du matériel utilisé en situation de nomadisme 18](#_Toc165297922)

[1.9. Plan de continuité d’activité – PCA 18](#_Toc165297923)

[PCA 01 : Plan de Continuité d’Activité 18](#_Toc165297924)

[PCA 02 : Test du plan de continuité d’activité 18](#_Toc165297925)

[1.10. Sécurité des astreintes - ASTR 19](#_Toc165297926)

[ASTR 01 : Sécurité des astreintes 19](#_Toc165297927)

[1.11. Sécurité lors de la réversibilité - REV 19](#_Toc165297928)

[REV 02 : Destruction des données en fin de prestation 19](#_Toc165297929)

[REV 03 : Phase de transfert 19](#_Toc165297930)

[1.12. Sécurité METIER - MET 19](#_Toc165297931)

[MET 01 : Sécurité des mises en production 19](#_Toc165297932)

# Exigences de sécurité

Pour chacune des exigences de sécurité concernées, des précisions et exemples de preuves attendues lors d’audits vous sont présentés afin de vous aider dans la complétion du PACS.

## **Cadre juridique - JUR**

JUR 01 : Réglementation spécifique

|  |
| --- |
| Exemples de preuves attendues lors des audits et contrôles :  - Durée de conservation des données  - Mécanismes d'archivage  - Mesures de protection associées |

JUR 02 : Localisation géographique des services et des données

|  |
| --- |
| Précisions :  Toute connexion aux Systèmes d’informations du groupe SNCF peut se faire à partir d’un pays de l’Union Européenne (toute connexion en dehors de l’Union Européenne est interdite).  Toutes les données du Client et les services du Prestataire ou de ses sous-traitants sont traitées exclusivement en Union Européenne  Dans le cadre de sa prestation, le Prestataire devra préciser :  - La liste exhaustive des lieux géographique de l’ensemble des services utilisés dans le cadre de la prestation (support, développement, hébergement, etc.)  - Les principes de remontée d’informations au Client en cas de modification en cours de contrat de localisation des lieux |
| Exemples de preuves attendues lors des audits et contrôles :  - Numéros de SIRET des établissements concernés  - Procédure de remontée d'informations vers le Client en cas de modification des lieux. |

JUR 03 : Certifications du Prestataire

|  |
| --- |
| Précisions :  Préciser les certifications détenues et incluses dans le périmètre de la prestation ainsi que :  - La date du prochain contrôle  - Le périmètre défini |
| Exemples de preuves attendues lors des audits et contrôles :  - Certifications  - Périmètres certifiés  - Rapports de certification (si diffusables) |

JUR 04 : Répercussion des clauses sur les sous-traitants

|  |
| --- |
| Précisions :  Indiquer la liste des sous-traitants amenés à intervenir sur la prestation.  Décrire comment les clauses du présent PACS sont appliquées et contrôlées auprès des sous-traitants du Prestataire. |
| Exemples de preuves attendues lors des audits et contrôles :  - Raison sociale des sous-traitants  - Dispositifs contractuels et opérationnels de répercussion des clauses du présent PACS auprès des sous-traitants (contrat, PACS, convention, etc.)  - Procédure de remontée d'informations vers le Client en cas de modification, en cours de contrat, de la liste des sous-traitants |

## **Organisation de la sécurité – ORG**

ORG 01 : Responsabilités et rôles sécurité

|  |
| --- |
| Précisions :  Le Prestataire précisera l’identité et les coordonnées de son correspondant sécurité ainsi que de son suppléant pour le Client (Nom, Prénom, Fonction, Téléphone, Mail).  Dans le cadre d’une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence), ces coordonnées doivent être également renseignés dans l’annexe 1 – BC2.  Le nom et les coordonnées seront fournis dans l’annuaire de la prestation, ses rôles et missions seront détaillés dans le PQS/PAQ ou document équivalent.  Ce correspondant est notamment :   * L'interlocuteur privilégié du Client pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d’investigations initiées par le Client ou par le Prestataire, à la suite d’incidents de sécurité opérationnels ; * Chargé du maintien et de la mise en application du PACS. |
| Exemple 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/PAQ, support de sensibilisation et Annexe 1). |

ORG 02 : Pilotage de la SSI

|  |
| --- |
| Précisions :  Les aspects sécurité (instances, fréquence, indicateurs, CR, acteurs, etc.) pourront être formalisés dans un PQS (Plan de Qualité de Service) ou PAQ (Plan d’Assurance Qualité) ou tout document équivalent. |
| Exemples de preuves attendues lors des audits et contrôles :  - PQS ou document équivalent validé  - Validation de la gouvernance sécurité par le Client (mail, compte-rendu, document version validée) |

ORG 03 : Détection, alerte et traitement des incidents de sécurité

|  |
| --- |
| Précisions :  Le processus formalisé et opérationnel de gestion des incidents de sécurité devra tenir compte des phases suivantes :   * Détection (en prenant le cas d’une détection par le Client et le cas d’une détection par le Prestataire), * Analyse, * Traitement * Alerte du Client   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 SI 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 le Client (bénéficiaire de la prestation) du processus de gestion des incidents de sécurité (mail, compte-rendu, document version validée) |

ORG 05 : Gestion de crise sécurité

|  |
| --- |
| 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(s) de crise (adresse postale, numéro de salle), moyens de télécommunication, annuaire) * Validation par le Client (bénéficiaire de la prestation) du plan de gestion de crise (mail, compte-rendu, document version validée) * Compte-rendu d'exercice de crise |

ORG 06 : Engagement Individuel de Confidentialité (EIC)

|  |
| --- |
| Précisions :  L’EIC a pour vocation de renforcer la sensibilisation des salariés ou personnes intervenant pour le compte du Prestataire ; ceux-ci s’engagent directement vis-à-vis du Prestataire qui reste responsable du respect des obligations de confidentialité. Une copie de chaque EIC sera remise à chacune des parties. |
| Exemples de preuves attendues lors des audits et contrôles :   * Engagements Individuels de Confidentialité signés * Dans le cadre d’une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence) : Document opérationnel de suivi des signatures (Annexe 1 ou autre document support) |

ORG 07 : Sensibilisation des intervenants à la sécurité informatique

|  |
| --- |
| Précisions :  Le Prestataire organise à sa charge la sensibilisation appropriée pour garantir le respect de cette mesure. |
| 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...) * Politique formalisée de nomadisme contenant les bonnes pratiques et les règles du travail en situation de nomadisme |

ORG 08 : Sensibilisation des intervenants au SI SNCF

|  |
| --- |
| 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 du Client seront fournies au démarrage de la Prestation par le Client, notamment sous forme de documentation.  Les documents sont fournis au Prestataire en même temps que le présent PACS.  La sensibilisation devra notamment traiter des sujets suivant :   * L'organisation sécurité de la prestation * La Charte de l'utilisateur pour l'usage du SI du Client * La Charte administrateur pour l’administration du SI du Client * Protection du patrimoine informationnel du Client * Le respect de la confidentialité tel que défini au contrat * Le signalement des incidents de sécurité ou des suspicions d’incidents de sécurité |
| 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 SI du Client édictées dans les documents réalisés par les parties (PQS, plan de crise, etc.) pour la prestation et ceux fournis par le Client (PACS, chartes SI, Gouvernance sécurité, etc.) * Document opérationnel de suivi des signatures (Annexe 1 ou autre document support) * Attestations individuelles de suivi de formation ou feuilles d'émargement. * Politique formalisée de nomadisme contenant les bonnes pratiques et les règles du travail en situation de nomadisme |

ORG 09 : Identification de suppléants des personnels clés

|  |
| --- |
| Précisions :  Le Prestataire est en mesure d’assurer que l’absence d’une personne contribuant à la prestation n’engendrera pas de détérioration de la prestation. Pour cela, les personnes ayant des fonctions clefs et leurs suppléants ont été clairement identifiés. |
| Exemple de preuves attendues lors des audits et contrôles :  - Liste des personnes expertes ou décideuses et de leurs suppléants |

## **Audit et Contrôles de sécurité - CTRL**

CTRL 01 : Autocontrôle de sécurité

|  |
| --- |
| Précisions :  Les modalités de restitution des autocontrôles de conformité sont à définir avec le Client avant le démarrage de la prestation.  Exemple de Tableau de bord sécurité : |
| Exemple de preuves attendues lors des audits et contrôles :  - Tableau de bord sécurité d'autocontrôle complété ou résultats de l'autocontrôle |

CTRL 02 : Contrôles de sécurité du SI

|  |
| --- |
| Précisions :  A noter que dans cette exigence, sont entendus notamment que :   * Le rapport sera fourni au Client * Le Prestataire s'engage à collaborer de bonne foi avec le Client |
| 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 |

CTRL 03 : Auditabilité du PACS

|  |
| --- |
| Précisions :  Le Prestataire spécifiera ici son accord ainsi que les modalités d'exécution et un délai de prévenance (proposé 5 jours) s'ils ne sont pas précisés au contrat.  Sont entendus notamment que :   * Le rapport sera fourni au Client * Le Prestataire s'engage à collaborer de bonne foi avec le Client   Le coût des contrôles est supporté par le Client. Toutefois, le coût induit par la participation aux contrôles d’intervenants du Prestataire reste à la charge de celui-ci. |
| 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 |

CTRL 04 : Sécurité des outils et services

|  |
| --- |
| Précisions :  Liens vers les dispositifs de vérifications cités dans l’exigence :   * [Application Security Verification Standard (ASVS)](https://owasp.org/www-project-application-security-verification-standard/) * [Mobile Application Security Verification Standard (MASVS)](https://owasp.org/www-project-mobile-security-testing-guide/)   Le Prestataire décrit ici les dispositifs mis en place pour assurer la détection des vulnérabilités |
| Exemple de preuves attendues lors des audits et contrôles :   * Rapport des contrôles effectués au minimum une fois par an. |

CTRL 05 : Contrôle des connexions d’administration distantes

|  |
| --- |
| Exemples de preuves attendues lors des audits et contrôles :  - Rapport des audits réalisés  - Rapport des scans de vulnérabilités des connexions à distance effectuées |

CTRL 06 : Correction des écarts identifiés

|  |
| --- |
| Précisions :  Les retards pourront donner lieu à des pénalités financières (selon le contrat en vigueur). |
| Exemples de preuves attendues lors des audits et contrôles :  - Plan d'actions de mise en conformité des écarts constatés lors des audits  - Fourniture du plan d'actions dans les 15 jours suivant la constatation des écarts (date de remise du plan d'actions (mail, etc.) |

## **Sécurité des environnements - ENV**

ENV 02 : Protection contre les programmes malveillants

|  |
| --- |
| Précisions :   * Décrire les anti-virus et les systèmes de protection utilisés contre les codes malveillants présents sur ses équipements (postes de travail et serveurs notamment). * Décrire la fréquence de mise à jour des bases anti-virales (min. : quotidienne) et la fréquences des scans de ressources (min. : hebdomadaire). * 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 (consigné dans l'Annexe 1) 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 signatures 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) |

ENV 03 : Suivi de la protection contre les programmes malveillants

|  |
| --- |
| Précisions :  Décrire la procédure de suivi hebdomadaire du bon déploiement des mises à jour antivirales (récupération des signatures antivirales, déploiement, récupération des journaux de déploiement des signatures, plan d’actions 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, révision de niveau de 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 |

ENV 04 : Maintien en condition de sécurité

|  |
| --- |
| Précisions :  Décrire le système de déploiement et de surveillance des correctifs de sécurité sur les composants logiciels et techniques de la prestation ( postes de travail, serveurs, équipements réseau, logiciels, firmwares, librairies, etc.). En précisant pour chaque type de ressource : les systèmes d’exploitation, éditeurs, fréquences de déploiement, etc.  Sont concernés :   * 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   Un délai de mise en place des mises à jour de sécurité de 3 mois est ponctuellement toléré pour les failles de sécurité ayant un score CVSS inférieur à 5.  Dans le cas d’utilisation du BYOD, l'ensemble des postes peuvent par exemple être gérés par un outil de type MDM |
| Exemples de preuves attendues lors des audits et contrôles :  - Description du dispositif permettant le déploiement et la surveillance des correctifs de sécurité (Unix/Windows) 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 |

ENV 05 : Suivi de l'application des correctifs de sécurité

|  |
| --- |
| Précisions :  Décrire la procédure de suivi du bon déploiement des correctifs de sécurité (récupération des journaux de déploiement, plan d’actions 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 |

## **Sécurité des données - DATA**

DATA 01 : Classification des données

|  |
| --- |
| Précisions :  « Personnes ayant le Besoin d’en connaître » : i.e. personnes qui auront potentiellement accès aux données de la prestation et qui doivent être conscientes 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 du Client). Cette classification est fournie par le Client au Prestataire au démarrage de la prestation.  La communication de la classification des données doit être faite à l’entrée du personnel du Prestataire et à chaque modification du périmètre applicatif.  Le Prestataire demandera au Client la classification des données avant le démarrage des services et à chaque modification du périmètre applicatif. |
| Exemples de preuves attendues lors des audits et contrôles :  - Trace de réception de la classification des données par le Client (mail, etc.). En l'absence de classification, le niveau de classification globale est celui défini par les Référentiels RA00110 et RRA20004.  - 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. |

DATA 02 : Gestion des données

|  |
| --- |
| Précisions :  Les synthèses des Référentiels RA00110 et RRA20004 sont fournis en document de référence en même temps que le présent PACS. |
| 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 les Référentiels RA00110 et RRA20004 :  - Impression  - Destruction  - Stockage  - Diffusion/reproduction  - Échange (mail/courrier)  - Photos des dispositifs |

DATA 03 : Cloisonnement des données du Client

|  |
| --- |
| Précisions :  Décrire :  - les moyens de cloisonnement prévus pour la protection des données du Client  - les engagements en termes de non-utilisation des données en dehors des environnements prévus dans le contrat.  Cette exigence couvre les données propriété du Client et également celles :  - hébergées sur des serveurs de fichiers et de messagerie du Prestataire  - produites pour le Client (livrables) |
| Exemples de preuves attendues lors des audits et contrôles :  - Schéma d’architecture  - Configuration des VLAN  - GPO, ACL, etc.  - DAT |

DATA 04 : Sauvegarde des données

|  |
| --- |
| 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 connaissances dédiée aux informations de connexion administrateurs (identifiants + mots de passe) aux différentes ressources -> A faire définir par la MOA lors de la qualification du PACS |
| 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 |

DATA 05 : Restauration des sauvegardes

|  |
| --- |
| Précisions :  Décrire la procédure de test de restauration (périmètre, fréquence, comptes rendus, plan d’actions 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 (journaux d’évènements, compte-rendu, PV) |

DATA 06 : Stockage des sauvegardes

|  |
| --- |
| 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 vers 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 hébergeant les sauvegardes |

## **Sécurité des accès logiques - SAL**

SAL 01 : Identifiants du Prestataire

|  |
| --- |
| 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.)  Les comptes administrateur par défaut doivent être renommés.  Les comptes invités doivent être désactivés. |
| 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 |

SAL 02 : Identifiants du Client sur le SI Prestataire

|  |
| --- |
| Précisions :  Pour répondre à cette exigence, le Prestataire privilégiera les solutions de raccordement au SI du Client, type Fédération d’Identité exploitant les informations (identifiants / jetons / privilèges) issues de l’annuaire du Client.  S’il utilise une solution sans raccordement, le Prestataire explicite comment sont opérées les identités : création / modification / suppression et qui est le garant de ce processus.  Le Prestataire pourra éventuellement utiliser une solution sans raccordement. Il explicitera 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 termes de gestion des identifiants du Client sur les ressources de la prestation ;  - Procédure de la prestation de gestion des identifiants du Client (création/suppression/ modification). |

SAL 03 : Authentification du Prestataire en administration

|  |
| --- |
| Précisions :  Décrire la politique de mot de passe. Préciser les éventuelles procédures d’accès distant. |
| Exemples de preuves attendues lors des audits et contrôles :  - Politique de mot de passe des intervenants dont les administrateurs fonctionnels et techniques du Prestataire utilisée dans le cadre de la prestation  - Capture d'écran des politiques de mot de passe implémentées (ex GPO sous Windows) sur les serveurs, équipements réseau et postes de travail (comptes administrateurs) indiquant :  1) La robustesse du mot de passe en termes de longueur et de complexité suivant les quatre familles de caractères disponibles  2) La durée de vie du mot de passe  - 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 prolongée sur les ressources de la Prestation |

SAL 04 : Existence d’un bastion pour se connecter en administration

|  |
| --- |
| Un bastion d’administration est un élément du réseau informatique permettant de fournir un point d’accès unique aux ressources via un flux chiffré et sécurisé. Le bastion fait office de proxy sécurisé entre les ressources et les utilisateurs qui ont besoin d’y accéder.  Un bastion permet notamment d’assurer la traçabilité de l’ensemble des connexions et des actions réalisées sur le SI par les titulaires des comptes à privilèges. |

SAL 05 : Gestion des privilèges

|  |
| --- |
| Précisions :  Décrire les différentes typologies de profils existantes et les droits associés ainsi que les processus mis en place pour s’assurer que ces droits 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 : principe 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 |

SAL 06 : Revue et suivi des comptes du domaine de responsabilités du Prestataire

|  |
| --- |
| Précisions :  Décrire les procédures de revue sur les ressources du SI du Prestataire (postes de travail, serveurs, équipements réseaux) : modes opératoires, périodicités, responsabilités, plan d’actions 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 quitté 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 |

SAL 07 : Traçabilité des accès logiques

|  |
| --- |
| Précisions :  Décrire le dispositif de traçabilité des accès aux ressources du SI Prestataire (contenu des journaux d’évènements, sauvegarde des journaux d’évènements, localisation des sauvegardes, durée de conservation, exploitation éventuelle des journaux d’évènements etc.)  Les ressources du SI 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 du Client de ces enregistrements.  - Exemple de trace (avec au moins identifiant, date/heure, action(s) réalisée(s) et statut de la connexion) au niveau des ressources de type système et applicatif. |

SAL 08 : Suivi des mécanismes de traçabilité des accès logiques

|  |
| --- |
| 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’actions 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 opérationnel du bon enregistrement des traces |

SAL 09 : Suivi du personnel du prestataire

|  |
| --- |
| Précisions :  Le Prestataire doit tenir à jour un registre de son personnel intervenant dans le cadre de la prestation. Dans le cadre d’une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence) ce registre est établi sur le modèle de l’Annexe 1 – BC2.  Indiquer votre engagement à participer aux revues périodiques de comptes du SI du Client 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 SI du Client.  Dans le cadre d’une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence) les revues seront tracées dans l’Annexe 1 du présent PACS.  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 quitté 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 droits nécéssaires pour mener à bien leurs missions.  Le Prestataire s'assurera auprès du Client de la réalisation de revues périodiques\* des comptes d’accès aux ressources informatiques (serveurs, postes de travail, applications) du Client utilisées dans le cadre de la prestation. |
| Exemples de preuves attendues lors des audits et contrôles :  - Procédure d’accès au SI du Client (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  - Dans le cadre d’une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence) : Annexe 1 à jour |

## **Sécurité réseau - RES**

RES 01 : Politique de gestion des flux réseau

|  |
| --- |
| Précisions :  Décrire les règles de filtrage des équipements réseau. |
| 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 » |

RES 02 : Cartographie des flux

|  |
| --- |
| 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)  - CR de la dernière revue de la matrice de flux  - DAT |

RES 03 : Interconnexion au SI du Client

|  |
| --- |
| Précisions :  Décrire l’architecture et les moyens retenus pour le cloisonnement de son SI pour éviter tout rebond sur le SI du Client (VLAN, équipements dédiés, etc.).  En complément de cet engagement, fournir le DAT.  L’architecture d'interconnexion doit être validée en comité de validation de l’architecture. |
| Exemples de preuves attendues lors des audits et contrôles :  - Schéma d’architecture de la prestation (interconnexion, serveurs hébergeant des données du Client, serveurs d’infrastructures, équipements réseau, postes de travail, connexion nomade, astreintes, protocoles des flux réseaux, systèmes d’exploitation utilisés sur les équipements, représentation des sites et adresses de ceux-ci, etc.).  - Preuve de validation de l’architecture de la prestation par le Client (Comité des Accès Externes (CAE))  - Éventuels schémas d’architecture de la prestation en mode dégradé en explicitant les scénarios de risques  - DAT |

RES 05 : Chiffrement des flux

|  |
| --- |
| Précisions :  Décrire les moyens de chiffrement de flux prévus sur le périmètre de la Prestation, dont au minimum :   * Tous les flux d’authentification des utilisateurs et des administrateurs * Tous les flux relatifs à des accès distant * Tous les flux spécifiquement mentionnés au contrat. |
| 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)  - DAT |

RES 06 : Prévention contre les attaques externes

|  |
| --- |
| 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, 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) |

RES 07 : Traçabilité des accès réseau

|  |
| --- |
| Précisions :  Décrire le dispositif d’enregistrement des traces des équipements réseau (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 réseau  - Exemple de trace réseau d’une transaction sur le périmètre de la prestation |

RES 08 : Suivi des mécanismes de traçabilité des accès réseau

|  |
| --- |
| 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’actions 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 opérationnel du bon enregistrement des traces |

## **Sécurité physique - PHYS**

PHYS 01 : Contrôle des accès physiques aux locaux du Prestataire

|  |
| --- |
| 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).  La procédure de gestion des accès physiques doit préciser au minimum les modalités de gestion des demandes et suppressions d’accès ainsi qu'une revue trimestrielle. |
| 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 |

PHYS 04 : Contrôle des accès physiques aux ressources techniques du Prestataire

|  |
| --- |
| 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 |

PHYS 05 : Protection contre les intrusions physiques dans les locaux hébergeant les ressources techniques du Prestataire

|  |
| --- |
| 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 de 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 |

PHYS 06 : Certification des sites d'hébergement des ressources techniques

|  |
| --- |
| Précisions :  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. |
| 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) |

PHYS 07 : Protection contre les évènements environnementaux

|  |
| --- |
| 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) |

PHYS 08 : Plan de maintenance

|  |
| --- |
| Exemples de preuves attendues lors des audits et contrôles :  - Plan de maintenance des infrastructures (personne en charge de la maintenance, société tiers intervenant dans le cadre de la maintenance)  - Exemple de contrat ou d’intervention de maintenance |

PHYS 09 : Protection contre le vol du matériel

|  |
| --- |
| Précisions :  Sont entendus ici les matériels du Client sous la responsabilité du Prestataire et les matériels Prestataire utilisés dans le cadre du contrat (traitant les données du Client).  Par terminaux mobiles sont entendus : postes de travail, ordinateurs portables, tablettes, téléphones.  Le Prestataire s'engage notamment à mettre en place des câbles antivol sur les postes de travail de façon systématique.  Quelques exemples de mesures de sécurité (bonnes pratiques, câble antivol, armoire fermée, baie de stockage, digicode, accès restreint, …). |
| 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, géolocalisation, etc.) |

PHYS 10 : Sécurisation du matériel utilisé en situation de nomadisme

|  |
| --- |
| Précisions :  Le Prestataire met en place diverses mesures de sécurité (bonnes pratiques, dédie le matériel utilisé en situation de nomadisme à un utilisateur nomade identifié, …). Cette exigence concerne le matériel fourni par le Client et le matériel du prestataire. |

## **Plan de continuité d’activité – PCA**

PCA 01 : Plan de Continuité d’Activité

|  |
| --- |
| Précisions :  Le PCA doit contenir au minimum :   * Le périmètre couvert par le Prestataire * Le niveau de continuité de service fourni (par exemple : DIMA, PDMA...) * Les scénarios de sinistre pris en compte * Les solutions de secours mises en œuvre * Les procédures opérationnelles de secours associées   Les scénarios attendus, s'ils sont applicables, peuvent notamment être :  - Indisponibilité partielle ou totale du personnel 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 SI du Prestataire utilisées dans le cadre de la prestation  DIMA (Durée Interruption Maximal Admissible)  PDMA (Perte de Données Maximale Admissible) |
| Exemples de preuves attendues lors des audits et contrôles :  \* Le PCA 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 |

PCA 02 : Test du plan de continuité d’activité

|  |
| --- |
| 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. |

## **Sécurité des astreintes - ASTR**

ASTR 01 : Sécurité des astreintes

|  |
| --- |
| Précisions :  Une astreinte est une période durant laquelle un intervenant, sans être sur son lieu de travail (comprenant le lieu de la prestation) et sans être à la disposition permanente et immédiate du Client et de son employeur, doit être en mesure d’intervenir pour accomplir un travail au service de la prestation.  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 du Client  - Toute modification de l’architecture de la prestation doit être soumise à la validation du Client. |
| 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 le Client |

## **Sécurité lors de la réversibilité - REV**

REV 02 : Destruction des données en fin de prestation

|  |
| --- |
| Précisions :  Décrire la procédure de transfert et de destruction utilisée sur le périmètre de la prestation :   * Les modalités et délais de restitution des données * La destruction des données présentes sur tous les environnements (production, pré-production, qualification, développement…) * La destruction des données présentes sur des supports de sauvegardes, même si ceux-ci sont mutualisés.   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) |

REV 03 : Phase de transfert

|  |
| --- |
| Précisions :  Durant la phase de transfert, l’assurance de la sécurité résidera principalement dans :   * La gestion des accès, habilitations ; * Le transfert de responsabilités ; * La fourniture d’informations confidentielles ; * La gestion de la continuité de l’activité. |

## **Sécurité METIER - MET**

MET 01 : Sécurité des mises en production

|  |
| --- |
| Précisions :  A noter que toute modification d'un environnement de production, effectuée par le personnel du Prestataire, devra avoir été préalablement validée par le Client (processus de gestion des changements, comité de validation, suivi des implémentations). |