|  |
| --- |
|  |
| PLAN D’ASSURANCE CYBER-SECURITE (PACS) [PRESTATION] – [PRESTATAIRE] |
| Bénéficiaire : Groupe SNCF Intitulé Prestation : [PRESTATION]Société Prestataire : [Prestataire] |
| Référence | PLAN D’ASSURANCE CYBER SECURITE [PRESTATION] – [PRESTATAIRE] |
| Version du modèle PACS utilisé | PG 1.6.1 |
| Version du document | 1.0 |
| Statut du document | VERSION DE TRAVAIL |
| Date de dernière modification | [DATE] |
| CONTRAT | [NUMERO DE CONTRAT] |

Cadre de validation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | version | nom | Fonction | Action |
| [DATE] | 1.0 | [Rédacteur] | Membre du pôle PACS | Rédaction |
| [DATE] | 1.0 | [RCS] | RCS | Vérification |
| [DATE] | 1.0 | [RCS | RSSI] | RCS | RSSI | Validation |

**CONFIDENTIEL SNCF**

En application des règles de classification SSI du Groupe SNCF, ce document est strictement réservé aux personnes habilitées pour le connaître.

|  |  |
| --- | --- |
| SNCF - sécurité du système d’information | Logo du groupe SNCF |

Historique des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| Date de la modification | Version de référence | Objet et Description de la modification | Chapitres modifiés |
| [DATE] | 1.0 | Création – Modification - … |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Liste de diffusion

|  |  |
| --- | --- |
| Destinataire | Objet de la diffusion (application, information, archivage, …) |
|  Intervenants qualifiés | APPLICATION / INFORMATION |
| Membres de la fonction sécurité SI | APPLICATION / INFORMATION |
| Responsable Référentiel SSI | ARCHIVAGE |

Documentation associée

|  |  |  |
| --- | --- | --- |
| Référence | TITRE du document | MOTIF |
| Synthèse RA00110 | Politique Thématique Sécurité SIProtection du Patrimoine Informationnel | APPLICABLE hors SNCF RÉSEAU |
| Synthèse RRA20004 | Politique Protection du Patrimoine Informationnel | APPLICABLE pour SNCF RÉSEAU |

Documents Annexes

|  |  |
| --- | --- |
| Référence | TITRE du document |
| Annexe 1 – BC2 | Personnel Prestataire |
| Annexe 2 | Précisions PACS Groupe SNCF 1.6.1 |

**Entre**

« Les parties » telles que définies au Contrat

Sommaire

[Préambule 7](#_Toc158393668)

[1. Presentation du document 8](#_Toc158393669)

[1.1. Objectifs 8](#_Toc158393670)

[1.2. Gestion du Plan d’Assurance Cybersécurité 8](#_Toc158393671)

[1.3. Responsabilité liée au PACS 9](#_Toc158393672)

[1.3.1 Entrée en application du PACS 9](#_Toc158393673)

[1.3.2 Processus d’évolution du PACS 9](#_Toc158393674)

[1.4. Application du PACS 10](#_Toc158393675)

[1.4.1 Applicabilité du PACS 10](#_Toc158393676)

[1.4.2 Cas de non-respect du PACS 10](#_Toc158393677)

[1.4.3 Dérogations 11](#_Toc158393678)

[2. Mode opératoire de réponse 12](#_Toc158393679)

[3. Engagement sur les accès au Système d’Information dU CLIENT 13](#_Toc158393680)

[3.1. Modifications, restrictions et interruption d’accès 13](#_Toc158393681)

[4. Description de la prestation ou du service 14](#_Toc158393682)

[4.1. Données utilisées dans le cadre de la prestation 14](#_Toc158393683)

[5. Exigences de sécurité 15](#_Toc158393684)

[5.1. Cadre juridique - JUR 15](#_Toc158393685)

[JUR 01 - Réglementation spécifique 15](#_Toc158393686)

[JUR 02 : Localisation géographique des services et des données 15](#_Toc158393687)

[JUR 03 : Certifications du Prestataire 16](#_Toc158393688)

[JUR 04 : Répercussion des clauses sur les sous-traitants 16](#_Toc158393689)

[5.2. Organisation de la sécurité – ORG 16](#_Toc158393690)

[ORG 01 : Responsabilités et rôles sécurité 16](#_Toc158393691)

[ORG 02 : Pilotage de la SSI 17](#_Toc158393692)

[ORG 03 : Détection, alerte et traitement des incidents de sécurité 17](#_Toc158393693)

[ORG 04 : Séparation des activités de développement 18](#_Toc158393694)

[ORG 05 : Gestion de crise sécurité 18](#_Toc158393695)

[ORG 06 : Engagement Individuel de Confidentialité (EIC) 18](#_Toc158393696)

[ORG 07 : Sensibilisation des intervenants à la sécurité informatique 19](#_Toc158393697)

[ORG 08 : Sensibilisation des intervenants au SI SNCF 19](#_Toc158393698)

[ORG 09 : Identification de suppléants des personnels clés 19](#_Toc158393699)

[5.3. Audit et Contrôles de sécurité - CTRL 20](#_Toc158393700)

[CTRL 01 : Autocontrôle de sécurité 20](#_Toc158393701)

[CTRL 02 : Contrôles de sécurité du SI 20](#_Toc158393702)

[CTRL 03 : Auditabilité du PACS 20](#_Toc158393703)

[CTRL 04 : Sécurité des outils et services 21](#_Toc158393704)

[CTRL 05 : Contrôle des connexions d’administration distantes 21](#_Toc158393705)

[CTRL 06 : Correction des écarts identifiés 22](#_Toc158393706)

[5.4. Sécurité des environnements - ENV 22](#_Toc158393707)

[ENV 01 : Utilisation du BYOD 22](#_Toc158393708)

[ENV 02 : Protection contre les programmes malveillants 22](#_Toc158393709)

[ENV 03 : Suivi de la protection contre les programmes malveillants 23](#_Toc158393710)

[ENV 04 : Maintien en condition de sécurité 23](#_Toc158393711)

[ENV 05 : Suivi de l'application des correctifs de sécurité 23](#_Toc158393712)

[ENV 06 : Chiffrement des postes de travail 24](#_Toc158393713)

[5.5. Sécurité des données - DATA 24](#_Toc158393714)

[DATA 01 : Classification des données 24](#_Toc158393715)

[DATA 02 : Gestion des données 24](#_Toc158393716)

[DATA 03 : Cloisonnement des données du Client 25](#_Toc158393717)

[DATA 04 : Sauvegarde des données 25](#_Toc158393718)

[DATA 05 : Restauration des sauvegardes 25](#_Toc158393719)

[DATA 06 : Stockage des sauvegardes 26](#_Toc158393720)

[DATA 07 : Chiffrement des données sensibles 26](#_Toc158393721)

[DATA 08 : Sécurité des données sur les environnements de développement 26](#_Toc158393722)

[5.6. Sécurité des accès logiques - SAL 27](#_Toc158393723)

[SAL 01 : Identifiants du Prestataire 27](#_Toc158393724)

[SAL 02 : Identifiants du Client sur le SI Prestataire 27](#_Toc158393725)

[SAL 03 : Authentification du Prestataire 28](#_Toc158393726)

[SAL 04 : Existence d’un bastion pour se connecter en administration 29](#_Toc158393727)

[SAL 05 : Gestion des privilèges 29](#_Toc158393728)

[SAL 06 : Revue et suivi des comptes du domaine de responsabilités du Prestataire 29](#_Toc158393729)

[SAL 07 : Traçabilité des accès logiques 29](#_Toc158393730)

[SAL 08 : Suivi des mécanismes de traçabilité des accès logiques 30](#_Toc158393731)

[SAL 09 : Suivi du personnel du prestataire 31](#_Toc158393732)

[5.7. Sécurité réseau - RES 31](#_Toc158393733)

[RES 01 : Politique de gestion des flux réseau 31](#_Toc158393734)

[RES 02 : Cartographie des flux 32](#_Toc158393735)

[RES 03 : Interconnexion au SI du Client 32](#_Toc158393736)

[RES 04 : Cloisonnement réseau des différents clients 32](#_Toc158393737)

[RES 05 : Chiffrement des flux 33](#_Toc158393738)

[RES 06 : Prévention contre les attaques externes 33](#_Toc158393739)

[RES 07 : Traçabilité des accès réseau 33](#_Toc158393740)

[RES 08 : Suivi des mécanismes de traçabilité des accès réseau 34](#_Toc158393741)

[5.8. Sécurité physique - PHYS 34](#_Toc158393742)

[PHYS 01 : Contrôle des accès physiques aux locaux du Prestataire 34](#_Toc158393743)

[PHYS 02 : Respect des normes de sécurité physiques et environnementales 34](#_Toc158393744)

[PHYS 03 : Locaux physiques dédiés aux prestations du Client 35](#_Toc158393745)

[PHYS 04 : Contrôle des accès physiques aux ressources techniques du Prestataire 35](#_Toc158393746)

[PHYS 05 : Protection contre les intrusions physiques dans les locaux hébergeant les ressources techniques du Prestataire 35](#_Toc158393747)

[PHYS 06 : Certification des sites d'hébergement des ressources techniques 36](#_Toc158393748)

[PHYS 07 : Protection contre les évènements environnementaux 36](#_Toc158393749)

[PHYS 08 : Plan de maintenance 36](#_Toc158393750)

[PHYS 09 : Protection contre le vol du matériel 37](#_Toc158393751)

[PHYS 10 : Sécurisation du matériel utilisé en situation de nomadisme 37](#_Toc158393752)

[PHYS 11 : Protection des plateaux mutualisés 37](#_Toc158393753)

[5.9. Plan de continuité d’activité – PCA 38](#_Toc158393754)

[PCA 01 : Plan de Continuité d’Activité 38](#_Toc158393755)

[PCA 02 : Test du plan de continuité d’activité 38](#_Toc158393756)

[5.10. Sécurité des astreintes - ASTR 38](#_Toc158393757)

[ASTR 01 : Sécurité des astreintes 38](#_Toc158393758)

[5.11. Sécurité lors de la réversibilité - REV 39](#_Toc158393759)

[REV 01 : Maintien de la sécurité durant la réversibilité ou transfert de la prestation 39](#_Toc158393760)

[REV 02 : Destruction des données en fin de prestation 39](#_Toc158393761)

[REV 03 : Phase de transfert 40](#_Toc158393762)

[5.12. SECURITE METIER – MET 40](#_Toc158393763)

[MET 01 : Sécurité des mises en production 40](#_Toc158393764)

[MET 02 : Règles de sécurité et d’exploitation 41](#_Toc158393765)

[MET 03 : Validité des sources d’installation des logiciels et des licences 41](#_Toc158393766)

[MET 04 : Test de non-régression des développements 41](#_Toc158393767)

[6. Récapitulatif des non-conformités 42](#_Toc158393768)

[7. Approbation 43](#_Toc158393769)

Préambule

En vertu du Contrat, les Parties sont convenues d’adopter le présent document (ci-après « PACS »), 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 en partie au « cloud computing » ;
* Centre de Services (CdS) ;
* Projet.

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.

Le Client sollicite le Prestataire pour la mise en place d’un partage d’informations unidirectionnel ou bidirectionnel, permettant aux employés habilités du Prestataire (ou de ses sous-traitants) de mettre à disposition une prestation ou un service localisé hors du système d’information du Client. Ce document règlemente les conditions d’échanges d’informations dans le cadre du Contrat. Dans le cas où le Prestataire dispose d’un accès au Système d’Information du Client soit pour y effectuer les activités, soit dans le cadre d’une connexion automatisée de l’objet de la prestation, les modes et conditions d’accès devront être décrits dans le Document d’Architecture Technique (DAT) ou documents équivalents (contrat, documentation technique, etc.).

Il est attendu de la part du Prestataire le respect des exigences de sécurité auxquelles il s’engage (exigences de sécurité ci-dessous) et des clauses de sécurité complémentaires du présent document. Les principes sont notamment issus de la norme ISO 27002 : 2013 et des recommandations de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI).

Par ailleurs, le présent PACS prend en compte la pratique du nomadisme dans ses exigences. La définition du nomadisme retenue est celle de l’ANSSI, à savoir « toute forme d’utilisation des technologies de l’information permettant à un utilisateur d’accéder au SI de son entité d’appartenance ou d’emploi, depuis des lieux distants, ces lieux n’étant pas maîtrisés par l’entité. ».

1. Presentation du document

Le présent document constitue le Plan d’Assurance Cyber Sécurité (PACS).

Il est entendu par « Assurance Cyber Sécurité » la garantie que la prestation se réalise dans les conditions de sécurité adaptées et garantissant un niveau d’assurance satisfaisant quant à la protection des données et des systèmes du périmètre du Client.

Ce document décrit ainsi les engagements relatifs à la sécurité établis entre le Client et le Prestataire dans le cadre de la Prestation et en particulier l’organisation à mettre en place, la méthodologie à suivre pour gérer la sécurité de la prestation, et les mesures physiques, organisationnelles, procédurales et techniques en réponse aux exigences de sécurité du Client.

Les contrôles et mesures définis dans ce PACS sont basés sur la Politique de Sécurité du Système d’Information (PSSI) de SNCF issue de la norme ISO 27002.

Dans la suite du présent document, sauf précision contraire :

* Le Prestataire [PRESTATAIRE] sera désigné par « Prestataire » ;
* La Prestation [PRESTATION] sera désignée par « Prestation »
* [LE CLIENT] sera désigné par « Le Client »
	1. Objectifs

Le Plan d’Assurance Cybersécurité de la Prestation constitue un référentiel pour le développement, le management et la garantie de la sécurité de la Prestation.

Il a pour objectifs de :

* Définir les normes, processus et procédures opérationnelles de sécurité à appliquer dans le cadre de la Prestation ;
* Fixer les responsabilités respectives entre le Prestataire et le Client, pour ce qui est de la sécurité ;
* Référencer les mesures prévues par le Prestataire associées au traitement et à la réduction des risques.

Chaque membre de l’équipe du Prestataire devra se conformer aux dispositions décrites dans ce Plan d’Assurance Cybersécurité.

* 1. Gestion du Plan d’Assurance Cybersécurité

Le présent document s’applique à la Prestation, pour laquelle toute ou partie de la sécurité de la réalisation ne peut être mise en place par le Client ; cette dernière sera en effet placée sous la responsabilité du Prestataire.

* 1. Responsabilité liée au PACS
		1. Entrée en application du PACS

Le Prestataire est chargé de compléter le PACS par la description des mesures de sécurité qu’il propose de mettre en œuvre face aux exigences du Client et permettant de s’assurer du respect des exigences de sécurité.

Le Prestataire doit :

* Décrire les dispositions de sécurité que le Prestataire applique pour assurer la sécurité de réalisation de la prestation conformément aux exigences de Sécurité définies par le Client ;
* Pour toutes dispositions déjà en vigueur chez le Prestataire car n’étant pas spécifique à
la Prestation, ce dernier peut simplement les mentionner dans le PACS et citer les
documents qui les décrivent. Ces documents doivent pouvoir être consultés sur simple
demande par le Client ;
* Décrire les mesures mises en place par le Prestataire pour répercuter les exigences
de sécurité du Client vers tous ses sous-traitants ;
* Préciser la date ou l’événement à compter duquel les dispositions de sécurité
décrites deviennent applicables.

Le Prestataire est chargé de diffuser et de faire appliquer le Plan d’Assurance Cybersécurité par les différents acteurs intervenant sur le projet (membres de l’équipe de développement, sous-traitants, cotraitants, partenaires, etc.).

Pendant la phase de contractualisation, le Prestataire complétera le PACS et le soumettra pour validation au Client.

Le PACS deviendra alors un document contractuel en tant qu’annexe au contrat de la prestation.

* + 1. Processus d’évolution du PACS

Le Prestataire se charge de retourner le PACS au Client pour toute demande de modification.

Le Client étudie les demandes de modifications du PACS. Tout refus de modification sera signalé au Prestataire. Le Client rédige la version finale du PACS et le transmet au Prestataire pour approbation.

Le Prestataire est chargé de transmettre la version finale du PACS aux acteurs concernés au sein de sa société de manière à pouvoir assurer l’approbation du document dans les délais fixés. Les délais seront fixés par le chef de projet du Client au moment de la transmission.

Toute modification du système d’information, de l’environnement du système d’information dans le périmètre de la Prestation ou de l’organisation proposée par le Prestataire est susceptible d’entraîner une évolution du PACS. Cette évolution peut se traduire par l’ajout, le retrait ou la modification des exigences de sécurité du PACS, en phase avec les besoins de la Prestation. Les évolutions du PACS seront réalisées par le responsable sécurité désigné par le Prestataire.

* + - 1. Revues périodiques

Une revue du PACS peut être organisée annuellement. Toute mise à jour du PACS décidée à la suite de cette revue donnera lieu à la création d’une nouvelle version majeure, approuvée et validée selon un processus identique à celui décrit pour la création du PACS.

Il est à la charge du Prestataire de proposer et organiser cette revue.

* + - 1. Évolutions ponctuelles

Il appartient au Prestataire de veiller à l’adéquation constante du PACS avec le niveau de sécurité attendu : toute modification du système d’information, de l’environnement du système d’information dans le périmètre de la Prestation ou de l’organisation proposée par le Prestataire pouvant affecter de manière directe ou indirecte le niveau général de sécurité devra être signalée au Client. Elle sera accompagnée si nécessaire des actions mises en œuvre afin de rétablir le niveau de sécurité attendu.

Lorsqu’une mise à jour du PACS est rendue nécessaire, notamment, par l’évolution du cadre réglementaire, technique, applicatif, ou par une modification de la Prestation, les éléments qui y sont décrits doivent être complétés ou mis à jour. De telles évolutions peuvent être à l’initiative du Client ou du Prestataire. Elles doivent être soumises au Client, qui peut les accepter ou les refuser.

Chaque évolution du PACS fera l’objet d’une évolution du numéro de version et sera tracée dans la fiche de suivi des versions du document.

Toute nouvelle version applicable sera formellement validée par le Client. Les éventuelles réserves seront explicitées.

Elle sera transmise au Prestataire, responsable de sa diffusion auprès des équipes et de son application.

* 1. Application du PACS
		1. Applicabilité du PACS

Le Plan d’Assurance Cybersécurité est applicable à l’ensemble des acteurs de la Prestation : il constitue un document contractuel lié à la Prestation.

Les dispositions décrites dans le PACS deviennent applicables dès le début de la prestation. Les versions ultérieures du PACS seront applicables dès leur validation par le Client.

Si l’une des parties constate un non-respect du Plan d’Assurance Cybersécurité, il devra le faire savoir à l’autre partie dans un délai d’au plus un mois après constatation.

Une non-conformité peut être :

* Acceptée de manière temporaire ; l’indication « Non conforme, dérogation » est une dérogation provisoire ; les conditions et délais de mise en conformité doivent être précisés dans un encart « Commentaire » positionné sous l’exigence ; le Prestataire doit faire évoluer sa solution ou son mode opératoire pour atteindre l’état « Conforme » ;
* Acceptée par le Client ; l’indication « Non conforme » n’oblige aucunement le Prestataire à changer sa solution ou son mode opératoire pour atteindre l’état « Conforme ». Cependant, les engagements pris dans l’encart « Commentaire » peuvent modifier les engagements pris par le Prestataire.

L’absence de positionnement de cette indication sur une exigence n’est pas possible.

* + 1. Cas de non-respect du PACS

En cas de non-respect du PACS, le Prestataire sera redevable du paiement de pénalités. Les modalités de calcul et d’application des pénalités sont précisées dans le contrat qui lie le Prestataire et le Client.

Lorsque la faute est considérée comme un manquement grave du Prestataire à son obligation de respecter le PACS, Le Client se réserve la possibilité de prononcer la résiliation du contrat.

Par ailleurs, Le Client se réserve le droit de suspendre les accès du Prestataire à son SI, si Le client estime que la sécurité de celui-ci est mise en danger par le non-respect d’une ou plusieurs mesures du PACS.

* + 1. Dérogations

Toute non-application du PACS ultérieure à sa signature conjointe doit être autorisée par le Client par le biais d’une dérogation formalisée.

La demande de dérogation au PACS doit être justifiée et soumise par le Manager du Prestataire au RSSI du Client.

Les dérogations sont validées par le responsable du métier concerné et par le RSSI du Client. En application de la PSSI du Client, une dérogation est limitée dans le temps.

Réciproquement, toute déviation par rapport au PACS constatée par le Prestataire et dont la proposition de remédiation est rejetée par le Client fera l’objet d’une demande formelle d’acceptation du risque (Risk Acceptance Agreement ou RAA) que le Prestataire soumet au Client. Ce document permet au Prestataire de s’assurer que le Client a formellement connaissance des risques identifiés que le Client encourt. Une telle dérogation ne peut dépasser un an selon la politique de sécurité du Client, mais peut être renouvelée si nécessaire.

1. Mode opératoire de réponse

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

Pour chaque exigence, le Prestataire :

* Coche les cases qui correspondent à ses engagements.
* Coche son niveau d’engagement (conforme ; non-conforme ou N/A).
* Décrit explicitement ses engagements dans la rubrique « Commentaire » lorsque cela est demandé ou si le Prestataire souhaite préciser des informations.
* Doit répondre aux exigences de la manière la plus explicite possible.
* Précise les éventuelles raisons d’une non-conformité, en fournissant des propositions alternatives ou 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 SI. Les éventuelles non-conformités seront soumises à l’étude des bénéficiaires de la prestation.
* Fournira les raisons liées au contexte de la prestation si une exigence est « Non Applicable ».

Une exigence engage le Prestataire sur la totalité des éléments définis dans l’exigence à moins que l’écart avec l’exigence ait été précisé en commentaire.

L’engagement du Prestataire sur une exigence du PACS emporte son acceptation sur l’ensemble du descriptif de l’exigence. Toute réserve sur une exigence du PACS doit être spécifiée en commentaire dans la case dédiée.

Ce document présente les différentes exigences sécurité de manière synthétique. Des précisions sur chaque exigence sont présentes dans l’annexe 2.

1. Engagement sur les accès au Système d’Information dU CLIENT
	1. 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, le Client peut modifier, restreindre ou interrompre à tout moment tout ou partie des accès à son Système d’Information, ce qui aurait pour conséquence pour le Client ou le Prestataire une impossibilité d’assurer tout ou partie des prestations ou services demandés. Le Client en avisera le Prestataire dans les meilleurs délais.

Le Client 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.

1. Description de la prestation ou du service

*Le Prestataire rappelle ici succinctement (en quelques lignes) l’objet du service ou de la Prestation et précise les éventuelles actions réalisées en nomadisme :*

*(À compléter par le prestataire)*

* 1. Données utilisées dans le cadre de la prestation

*Tableau complété par la SNCF :*

|  |  |  |
| --- | --- | --- |
| Typologie des données | Classification des données | Données personnelles (OUI/NON) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Date de la dernière modification du tableau : JJ/MM/AAAA*

1. 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. Pour plus de précisions sur les exigences, se référer à l’annexe 2.

* 1. Cadre juridique - JUR

JUR 01 - Réglementation spécifique

|  |
| --- |
| Le Prestataire s’engage à respecter toute réglementation spécifique liée à sa prestation (ex : RGPD, PCIDSS, HDS, etc.…).Si une réglementation particulière met en défaut le respect des exigences de sécurité du Client, alors le Prestataire doit :* Informer le Client 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 Client, en regard des évolutions fonctionnelles et techniques afférentes à cette réglementation.
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  | [ ]  Non Applicable  |
| Commentaire :  |

JUR 02 : Localisation géographique des services et des données

|  |
| --- |
| Le Prestataire s’engage à ce que toutes ses infrastructures (techniques ou organisationnelles) soient gérées au sein de l’Union Européenne (dont le Royaume-Uni et la Suisse), y compris en situation de nomadisme.Le Prestataire s’engage, sur le périmètre de la prestation, à spécifier dans le champ commentaire les lieux géographiques dans lesquels sont localisés :* Les données informatiques liées à la prestation
* Les services objets de la prestation
* Les personnes participant à la réalisation de la prestation (toute connexion en dehors de l’Union Européenne est interdite)

Le Prestataire s'engage à ne pas déplacer les données du Client sur un autre environnement que ceux définis dans la prestation, sans avoir préalablement reçu une autorisation formelle du Client.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  | [ ]  Non Applicable  |
| Commentaire :  |

JUR 03 : Certifications du Prestataire

|  |
| --- |
| Le Prestataire déclare disposer de certifications applicables sur le périmètre de la prestation (renseigner les certifications, leur périmètre et leur durée de validation en commentaires) et s’engage à fournir les justifications au Client.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  | [ ]  Non Applicable  |
| Commentaire :  |

JUR 04 : Répercussion des clauses sur les sous-traitants

|  |
| --- |
| Le Prestataire s’engage à répercuter les clauses du présent PACS dans ses contrats de sous-traitance et de cotraitance (actuels et futurs) et s’assurer de leur mise en œuvre effective.Le Prestataire précisera dans le champ commentaire les opérateurs (sociétés et fournisseurs) amenés à intervenir en cotraitance et sous-traitance.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

* 1. Organisation de la sécurité – ORG

ORG 01 : Responsabilités et rôles sécurité

|  |
| --- |
| Le Prestataire doit désigner parmi son personnel un correspondant sécurité pour toute la durée de la prestation (préciser toutes les coordonnées du correspondant (nom, prénom, titre, adresse électronique et numéro de téléphone) dans le champ commentaire).Ce correspondant doit être joignable aux horaires convenus dans le cadre contractuel (une suppléance doit être assurée pour pallier son indisponibilité).Tout remplacement de ce correspondant doit être notifié au Client préalablement à son entrée en vigueur.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire : Contact sécurité :NOM Prénom :Fonction :Mail :Tél :Suppléant :NOM Prénom :Fonction :Mail :Tél : |

ORG 02 : Pilotage de la SSI

|  |
| --- |
| Le Prestataire doit aborder les aspects sécurité dans le cadre de la gouvernance de la prestation. Ces points doivent être formalisés dans un document contractuel à faire valider par le Client avant le démarrage de la prestation. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

ORG 03 : 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. Le Prestataire s’engage à communiquer, dès qu’il en prend connaissance, tout évènement cyber ou incident de sécurité au CERT SNCF.Coordonnées du CERT SNCF :* Aux heures ouvrées : (mail) cert@sncf.fr ou (tél) 0 800 006 067
* Aux heures non ouvrées : (tél) 06 09 01 22 97

Le Prestataire doit permettre au Client de participer au traitement de l’incident si celui-ci impacte le périmètre de la prestation.Des réunions périodiques d’analyse post-incident devront être planifiées avec le Client pour le traitement des causes profondes.Toute modification du processus de gestion des incidents de sécurité doit être approuvée par le Client. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

ORG 04 : ~~Séparation des activités de développement~~

|  |
| --- |
| ~~Le Prestataire s’engage à ce que les ressources affectées aux activités de développement d’un projet soient différentes de celles réalisant la recette de ce même projet.~~~~Le Prestataire doit préciser si les équipes responsables de ses activités sont dédiées et doit décrire les moyens permettant de s'assurer qu'une activité ne peut pas être réalisée par une personne en charge d'une autre activité.~~ |
| **~~Engagement Prestataire :~~** |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

ORG 05 : 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. Le plan de gestion de crise doit intégrer les principes d'escalade, la composition de la cellule de crise et les moyens dédiés à la gestion de crise.Le plan de gestion de crise doit être présenté et validé par le Client. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

ORG 06 : Engagement Individuel de Confidentialité (EIC)

|  |
| --- |
| Le Prestataire s’engage à faire signer un engagement individuel de confidentialité (EIC) à ses salariés ou à toute personne intervenant dans l’exécution de la prestation et pouvant accéder à des données du Client. Dans le cadre d'une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence), le Prestataire s’engage à lister les intervenants ayant signé l’EIC dans l’annexe 1 - BC2, tenir à jour cette liste et la fournir sur demande au Client ou lors des comités de sécurité dédiés. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme |  |
| Commentaire :  |

ORG 07 : Sensibilisation des intervenants à la sécurité informatique

|  |
| --- |
| Le Prestataire doit organiser régulièrement des actions de sensibilisation à la sécurité de l’information pour son personnel.Le prestataire décrit en commentaire le type de formations réalisées ainsi que leur fréquence.Dans le cadre d'une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence), le Prestataire s’engage à tenir à jour l’annexe 1 – BC2 en y inscrivant les dates des sessions de sensibilisations. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

~~ORG 08 : Sensibilisation des intervenants au SI SNCF~~

|  |
| --- |
| ~~Le Prestataire s’engage à ce que chacun des intervenants sous sa responsabilité dans le périmètre de la prestation prenne connaissance des règles et politiques de sécurité qui leur seront transmises à leur arrivée.~~~~Cette sensibilisation doit être réalisée à la prise de poste du personnel du Prestataire, puis a minima annuellement ou en cas d'évolution des règles de protection du Système d’Information du Client.~~ ~~Le cas échéant, le Prestataire dispose d’une politique formalisée et d’un plan de sensibilisation lui permettant d’assurer une partie ou la totalité de la prestation en situation de nomadisme, et ce de manière sécurisée.~~~~Dans le cadre d'une prestation de type CdS (Centre de Service) ou CdC (Centre de Compétence), le Prestataire s’engage à tenir à jour l’annexe 1 – BC2 en y inscrivant les dates des sessions de sensibilisations.~~ |
| **~~Engagement Prestataire :~~**  |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

ORG 09 : Identification de suppléants des personnels clés

|  |
| --- |
| Le Prestataire doit identifier un suppléant pour chaque personnel expert et/ou décideur afin d’assurer une polyvalence et de permettre la continuité de service. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

* 1. Audit et Contrôles de sécurité - CTRL

CTRL 01 : Autocontrôle de sécurité

|  |
| --- |
| Le Prestataire doit effectuer des autocontrôles de conformité (au minimum annuellement) aux exigences du présent PACS pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation. Ces autocontrôles doivent être formalisées et communiqués sur demande au client.Le Client se réserve le droit de demander au Prestataire de réaliser à sa demande un autocontrôle de conformité (au maximum 3 fois par an). |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

CTRL 02 : Contrôles de sécurité du SI

|  |
| --- |
| Le Prestataire s'engage à autoriser le Client à réaliser des contrôles de sécurité (ex : « scan de vulnérabilités », « test d'intrusion informatique ») sur le SI du Prestataire.Le coût des contrôles est supporté par le Client. Toutefois, le coût induit par la participation d’intervenants du Prestataire aux contrôles reste à la charge de celui-ci.Le Prestataire précise le délai de prévenance accepté en commentaire.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

CTRL 03 : Auditabilité du PACS

|  |
| --- |
| Le Prestataire s'engage à autoriser le Client à auditer les clauses du présent PACS afin de vérifier la conformité de ces exigences. Le Prestataire précise le délai de prévenance accepté en commentaire.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

CTRL 04 : Sécurité des outils et services

|  |
| --- |
| Le Prestataire démontre que les outils et services mis à disposition du Client respectent des règles de développement sécurisé, notamment les 10 principales vulnérabilités définies par l'OWASP.Le Prestataire s’appuiera sur les dispositifs de vérification suivants pour tester le niveau de conformité des développements des applications Web et des développements des applications mobiles :* Application Security Verification Standard (ASVS)
* Mobile Application Security Verification Standard (MASVS)

A défaut, il devra décrire les mécanismes utilisés pour confirmer sa conformité.Le Prestataire s’assure également que les développeurs sont sensibilisés aux pratiques de développement sécurisé.Si le Prestataire ne teste pas lui-même le code qu’il développe pour la mise en place de ses services, il précise en commentaire qu’il s’engage à soumettre son code aux outils du Client. En cas de non-conformité constatée à la suite d’un audit sécurité des développements réalisés, le prestataire s’engage à corriger les vulnérabilités éventuelles à sa charge et dans les délais imposés par le projet. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

~~CTRL 05 : Contrôle des connexions d’administration distantes~~

|  |
| --- |
| ~~Le Prestataire doit mener à fréquence annuelle une analyse de vulnérabilités et un test d’intrusion pour chaque connexion distante, liée à des actions d'administration, utilisée dans le cadre de la Prestation (action sur le SI SNCF depuis le SI Prestataire ou action sur le SI prestataire en situation de nomadisme).~~~~Le Prestataire communiquera au Client les résultats des tests d'intrusion.~~ |
| **~~Engagement Prestataire :~~**  |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

CTRL 06 : Correction des écarts identifiés

|  |
| --- |
| En cas d’écarts constatés avec les exigences de sécurité contractuelles, ou en cas de manquement à la sécurité à la suite d’un audit ou d’un contrôle, un plan de remédiation devra être formalisé par le prestataire au plus tard 15 jours après la livraison du rapport.Ce plan devra être validé conjointement par le Prestataire et le Client. Le Prestataire devra ensuite régulariser ces écarts ou manquements par l'application du plan de remédiation dans un délai convenu d’un commun accord par les deux parties. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

* 1. Sécurité des environnements - ENV

~~ENV 01 : Utilisation du BYOD~~

|  |
| --- |
| ~~Seuls les matériels fournis par l’entreprise prestataire sont acceptés (Pas de matériel personnel).~~~~En cas d’utilisation du BYOD chez le Client (postes fournis par le Prestataire et non pas le Client), la connexion filaire au SI SNCF est interdite. Le Prestataire devra disposer d’un téléphone portable sur lequel il devra installer l’outil d’authentification forte utilisé par le Client pour garantir une authentification multi-facteurs quand nécessaire.~~~~L’ensemble des exigences présentes dans ce PACS sont applicables également en cas de BYOD.~~ |
| **~~Engagement Prestataire :~~**  |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

ENV 02 : 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.

Le Prestataire détaillera en commentaire les mécanismes en place. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

ENV 03 : Suivi de la protection contre les programmes malveillants

|  |
| --- |
| Le Prestataire s’engage à mettre en place et à formaliser un suivi périodique (au minimum hebdomadaire) de l’état de mise à jour des systèmes de protection des postes de travail et serveurs contre les programmes malveillants.Le prestataire décrit en commentaire le dispositif de suivi ainsi que sa fréquence. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

ENV 04 : Maintien en condition 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 (fréquence à préciser en commentaire). Il s’engage notamment à réaliser une veille technologique et à appliquer les correctifs de sécurité adéquats dans des délais adaptés à la prestation.Dans le cas où l’utilisation de matériel en situation de nomadisme est autorisée, le Prestataire doit activer des mécanismes de mise en quarantaine et de remédiation pour les équipements nomades non conformes aux mises à jour de sécurité (ex : appliquer les dernières mises à jour de sécurité, appliquer les correctifs de sécurité, déconnecter l’équipement du SI interne de l’entité ou du SI Client…).  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

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

|  |
| --- |
| Un suivi périodique de l’état de mise à jour des correctifs de sécurité des composants logiciels et techniques du Prestataire (définis dans ENV 04) doit être effectué et formalisé. Le Prestataire précise la fréquence en commentaire (min. : mensuel). |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

~~ENV 06 : Chiffrement des postes de travail~~

|  |
| --- |
| ~~Les disques durs des postes de travail utilisés par le Prestataire doivent être chiffrés avec un algorithme robuste (minimum AES 256 ou équivalent) conformément à la PSSI du Client.~~ |
| **~~Engagement Prestataire :~~**  |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

* 1. Sécurité des données - DATA

~~DATA 01 : Classification des données~~

|  |
| --- |
| ~~Le Prestataire demandera au Client la classification des données avant le démarrage des services et à chaque modification du périmètre applicatif (tableau en chapitre 4).~~ ~~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.~~ |
| **~~Engagement Prestataire :~~**  |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

~~DATA 02 : Gestion des données~~

|  |
| --- |
| ~~L’accès, le stockage, l’échange et la destruction des documents et données doivent être sécurisés dans le respect du Référentiel du Client (RA00110 sauf pour SNCF RESEAU : RRA20004).~~~~En cas de BYOD, le stockage de données du Client sur le matériel Prestataire doit être préalablement autorisé par le Client.~~  |
| **~~Engagement Prestataire :~~**  |
| ~~[ ]  Conforme~~ | ~~[ ]  Non conforme~~ | ~~[ ]  Non Applicable~~ |
| ~~Commentaire :~~  |

DATA 03 : Cloisonnement des données du Client

|  |
| --- |
| 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 du Client, et notamment assurer qu’elles ne sont d’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 contenant des données de production du Client, le Prestataire s’engage à mettre en œuvre et à maintenir un cloisonnement vis à vis de tout autre environnement. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

DATA 04 : 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 le Client
* 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 du Client vis-à-vis des autres données hébergées par le Prestataire
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

DATA 05 : 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 du Client

Le Prestataire précisera la fréquence de ces restaurations, au minimum semestrielle. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

DATA 06 : 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. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

DATA 07 : Chiffrement des données sensibles

|  |
| --- |
| Le Prestataire s’engage à ce que toutes les données du Client classifiées « Restreint », « Confidentiel » ou « Secret » (tableau en chapitre 4), soient stockées sur le SI du Prestataire de manière chiffrée (donnée chiffrée individuellement ou conteneur chiffré : préciser en commentaire) avec un algorithme robuste (minimum AES 256 ou équivalent : préciser la méthode en commentaire).Le Prestataire doit disposer d’une politique de gestion des clefs de chiffrement dont il précise le fonctionnement en commentaire. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

DATA 08 : Sécurité des données sur les environnements de développement

|  |
| --- |
| Le Prestataire devra, sauf contre-indication explicite du Client, utiliser des jeux de données anonymisées. Dans le cas où des données de production ne peuvent pas être rendues anonymes, le Prestataire doit garantir leur confidentialité : il est notamment attendu que les environnements de développement soient d’un niveau de sécurité équivalent aux environnements de production.Le Prestataire s’engage à n’utiliser aucune donnée de production dans les environnements hors production. Le Prestataire s’engage spécifiquement à ne pas utiliser de données à caractère personnel réelles lors des tests sur ses environnements hors production. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

* 1. Sécurité des accès logiques - SAL

SAL 01 : 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 explicite 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 « invité » doivent être désactivés. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

SAL 02 : Identifiants du Client sur le SI Prestataire

|  |
| --- |
| Sur le périmètre de la prestation, le Prestataire doit mettre en place une solution de raccordement au SI du Client, type SSO (Single Sign-On) / Fédération d’Identité exploitant les informations (identifiants / jetons / privilèges) issues de l’annuaire du Client. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

SAL 03 : Authentification du Prestataire

|  |
| --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des informations d’authentification.Cela se traduit notamment pour :* Les accès de ses intervenants hors-administration par :
	+ L’utilisation de mots de passe d’une longueur minimale de 12 caractères contenant au moins trois des quatre familles de caractères.
* Les accès de ses intervenants en administration par :
	+ L’utilisation de mots de passe d’une longueur minimale 20 caractères (ou entre 12 et 20 caractères avec l’utilisation d’une double-authentification) contenant les quatre familles de caractères (lettres minuscules, lettres majuscules, chiffres, caractères spéciaux).
* Les accès de l’ensemble de ses intervenants par :
	+ Une politique de renouvellement des mots de passe, imposant un changement au minimum annuel (365 jours).
	+ L’utilisation de systèmes d’authentification à plusieurs facteurs pour les accès distants. En cas d’absence d’accès distant, le préciser en commentaire
	+ Le blocage temporaire du compte après un certain nombre de tentatives de connexions infructueuses successives (maximum 15 tentatives)
	+ Les sessions (système ou applicatives) doivent être protégées par des mécanismes de verrouillage automatique en cas d'inactivité prolongée (au maximum après 15 minutes).

Le Prestataire précise en commentaire tout autre dispositif d’authentification utilisé.Si certaines des activités de la prestation sont autorisées en situation de nomadisme, un système d’authentification à plusieurs facteurs doit être mis en place. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

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

|  |
| --- |
| Sur le périmètre de la prestation, en cas d’accès distants en administration sur le SI utilisé dans le cadre de la prestation, le Prestataire s’engage à réaliser toutes les actions d’administration techniques via un outil de type bastion.Les actions d’administration doivent être tracées et l’intégrité de celles-ci doit être garantie.Les accès directs aux serveurs sont limités à des usages exceptionnels dans le cadre de la résolution d’un incident de sécurité. Le Prestataire s’engage à tenir informé le Client tout au long de la résolution de l’incident. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| ~~Commentaire :~~  |

SAL 05 : 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. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

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

|  |
| --- |
| Des revues périodiques des comptes d’accès aux ressources informatiques du Prestataire (serveurs, postes de travail, applications), utilisées dans le cadre de la prestation doivent être effectuées et formalisées.Il est notamment attendu du Prestataire qu’il réalise : * Une revue « d’emploi » au minimum trimestrielle
* Une revue de « besoin » au minimum annuelle
* Une suppression des comptes des intervenants au plus tard 48h après leur départ
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme |  |
| Commentaire :  |

SAL 07 : 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 des 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. Le Prestataire précise en commentaire les données tracées.L’intégrité de ces traces doit être garantie.Les traces doivent pouvoir être fournies sur demande du Client. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

SAL 08 : 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.

Le Prestataire décrit en commentaire le processus de suivi périodique du bon enregistrement des traces ou un dispositif d'alerte en cas de non-enregistrement.Le Prestataire s'engage à ne pas désactiver les dispositifs de traçabilité mis en place et dispose d’un plan d’action en cas d'échec de la collecte. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

~~SAL~~ ~~09 : Suivi du personnel du prestataire~~

|  |
| --- |
| ~~Pour des prestations de plus de trois mois, le Prestataire doit tenir à jour un registre de son personnel intervenant dans le cadre de la prestation, ce registre doit être communicable sur demande du Client.~~ ~~Pour des prestations de type CDS (Centre de Service) ou CDC (Centre de Compétence) ce registre du personnel intervenant dans le cadre de la prestation correspond à la complétion de l’annexe 1 - BC2.~~~~Les demandes liées aux accès du personnel du Prestataire au SI du Client (création, modification, suppression) doivent être centralisées :~~ * ~~Le Prestataire suivra la procédure d’accès au SI du Client, fournie par le Client, pour toute demande d’accès ou de modification de droits.~~
* ~~Tout personnel du Prestataire qui ne figure pas sur le registre ne disposera pas d'un compte d'accès au SI.~~
* ~~Les comptes (identifiants et mots de passe) fournis par le Client 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 doivent être notifiés au Client à chaque mouvement ou modification~~
* ~~Le Prestataire s’engage à tracer le matériel du Client sous sa responsabilité ou celle de ses intervenants.~~

~~Le Prestataire s'assurera auprès du Client de la réalisation de revues périodiques\* des comptes d’accès aux ressources informatiques du Client (serveurs, postes de travail, applications), utilisées dans le cadre de la prestation.~~~~\*une revue « d’emploi » (au minimum trimestrielle), une revue de « besoin » (au minimum annuelle).~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

* 1. Sécurité réseau - RES

RES 01 : Politique de gestion des flux réseau

|  |
| --- |
| Le Prestataire met en place une politique de gestion des flux réseau, à décrire en commentaire.Sur le périmètre de la prestation, le Prestataire s’engage à ce que tous les flux non explicitement autorisés soient interdits. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

RES 02 : 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 (image à insérer en commentaire)
* Maintenir à jour cette matrice des flux et informer le Client de toute évolution
* Transmettre cette matrice sur demande du Client.
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  | [ ]  Non Applicable  |
| Commentaire :  |

~~RES 03 : Interconnexion au SI du Client~~

|  |
| --- |
| ~~Si la prestation requiert une interconnexion entre le réseau du Client et le réseau informatique du Prestataire, alors celui-ci s’engage à proposer une architecture conforme aux prérequis SSI du Client. Cette architecture devra être formalisée au travers d’un Dossier d’Architecture Technique (DAT). Celui-ci décrira les outils, les équipements, la matrice des flux, les protocoles utilisés. Ce DAT devra être communiqué au Client pour faire l’objet d’une vérification sur le plan sécurité.~~~~En cas de modification de l’architecture, le DAT devra être mis à jour et faire l’objet d’une nouvelle vérification par le Client.~~~~Le Prestataire décrit en commentaire l’architecture et les moyens retenus pour le cloisonnement de son SI.~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

RES 04 : Cloisonnement réseau des différents clients

|  |
| --- |
| Le Prestataire s’assure que les connexions mises en œuvre dans le cadre de la prestation sont distinctes des connexions utilisées pour les autres clients ou les autres projets du Prestataire. Expliciter en commentaire les mesures mises en œuvre.  |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  | [ ]  Non Applicable  |
| Commentaire :  |

RES 05 : 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 (les décrire) 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
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

RES 06 : Prévention contre les attaques externes

|  |
| --- |
| Le Prestataire mettra en œuvre des dispositifs adaptés au contexte afin de prévenir les attaques informatiques (intrusions, dénis de service, brute force…) sur le SI utilisé dans le cadre de la prestation. Préciser notamment la présence ou l’absence de firewall, firewall applicatif, sondes IDS/IPS. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

RES 07 : 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 (a minima : IP émetteur et destinataire, date et heure), pendant une durée minimale de 6 mois ou en accord avec les exigences légales et réglementaires en vigueur.De plus elles doivent pouvoir être fournies sur demande du Client.Le Prestataire précise en commentaire les dispositifs assurant la traçabilité des accès réseau. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

RES 08 : Suivi des mécanismes de traçabilité des accès réseau

|  |
| --- |
| Le Prestataire doit s'assurer mensuellement du bon fonctionnement des dispositifs de traçabilité : * Collecte effective des traces de ses éléments réseau (bastion, firewall, switch, routeur, antivirus, sondes IDS/IPS, …) afin de les rendre exploitables
* Sauvegarde effective des traces.

Le Prestataire décrit en commentaire :* Les dispositifs de suivi et d’exploitabilité des traces ainsi que la fréquence de ce suivi.
* Les éléments permettant de réaliser une synthèse de l’état des différents éléments du réseau
* Les cas d’usage de son dispositif de gestion des traces qui remonte des incidents de sécurité
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

RES 09 : Infrastructure de clefs publiques - PKI

|  |
| --- |
| Le Prestataire doit s'assurer de passer par les autorités de certification autorisées par le Client pour générer les certificats SSL de sa prestation.Le prestataire s’engage à ne pas utiliser de certificats auto-signés.Le Prestataire décrit en commentaire :* L’autorité de certification qu’il utilisera dans le cadre de la prestation.
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

* 1. Sécurité physique - PHYS

PHYS 01 : 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 conservée 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. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

~~PHYS 02 : Respect des normes de sécurité physiques et environnementales~~

|  |
| --- |
| ~~Le Prestataire doit détailler en commentaire les mesures mises en œuvre afin de garantir la sécurité physique et environnementale des locaux hébergeant son personnel.~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

PHYS 03 : Locaux physiques dédiés aux prestations du Client

|  |
| --- |
| Le Prestataire dispose de locaux spécifiques, dédiés à la prestation du Client, isolés de ses autres locaux. Le personnel du Prestataire n’étant pas clairement identifié comme étant habilité à accéder à des données du Client ne doit pas pouvoir accéder à ces locaux dédiés. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 04 : 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. Le Prestataire décrit en commentaire ces dispositifs. 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. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 05 : 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. Le Prestataire précise en commentaire ces dispositifs.Les traces des évènements, des alarmes, des actions de traitement et de clôture doivent pouvoir être fournies sur demande du Client. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 06 : 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 lié à la prestation.Le Prestataire précise en commentaire les certifications des sites d’hébergement des ressources techniques ou le service lié à la prestation ou à défaut, les systèmes de protection et de surveillance en place contre les évènements pouvant perturber l’activité.Les traces des évènements, des alarmes, des actions de traitement et de clôture doivent pouvoir être fournies sur demande du Client. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 07 : Protection contre les évènements environnementaux

|  |
| --- |
| Le Prestataire décrira en commentaire les risques environnementaux dont font l’objet les sites hébergeant les données ou le service.En cas de risque avéré, le Prestataire précisera en commentaires les mesures mises en œuvre pour couvrir ces risques (plan de prévention des risques). |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 08 : Plan de maintenance

|  |
| --- |
| Un plan de maintenance des infrastructures (bâtiments, énergie, matériels informatiques, télécommunications, …) du Prestataire mises en œuvre dans le cadre de la prestation doit être défini et appliqué.Le Prestataire décrit en commentaire les moyens mis en œuvre pour satisfaire ce plan de maintenance des infrastructures (sous-traitants éventuels, risques identifiés et couverts…). |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 09 : Protection contre le vol du matériel

|  |
| --- |
| Le Prestataire met en place des dispositifs physiques afin d’assurer la sécurité du matériel sous sa responsabilité (postes de travail, serveurs, …). Ces dispositifs doivent prévenir les vols de terminaux mobiles et autres supports d’information (postes de travail, serveurs, clefs USB...).Si le Prestataire détient ou utilise du matériel prêté par le Client dans le cadre de la Prestation, le Prestataire s’engage à tracer dans l’annexe 1 le matériel du Client sous sa responsabilité ou celle de ses intervenants. Le Prestataire précise en commentaire ces dispositifs. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PHYS 10 : Sécurisation du matériel utilisé en situation de nomadisme

|  |
| --- |
|  |
| Le Prestataire met en place des mesures de sécurité techniques et organisationnelles afin d’assurer sous sa responsabilité la sécurité du matériel utilisé en situation de nomadisme. Pour cela il met en place diverses mesures de sécurité (bonnes pratiques, dédie le matériel utilisé en situation de nomadisme à un utilisateur nomade identifié, …) qu’il décrit en commentaire. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

~~PHYS 11 : Protection des plateaux mutualisés~~

|  |
| --- |
| ~~En cas de mutualisation de ses plateaux, le Prestataire devra mettre en place des mesures pour protéger les espaces attribués pour la prestation effectuée pour le Client (accès aux postes par badge, blocage automatique des sessions après un certain temps d’inutilisation, câble de sécurité pour le matériel fourni par le Client, etc.) qu’il décrira en commentaire.~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

* 1. Plan de continuité d’activité – PCA

PCA 01 : Plan de Continuité d’Activité

|  |
| --- |
| Un Plan de Continuité d’Activité (PCA) ou Plan de Continuité de Service (PCS) doit être défini, formalisé en conformité avec les besoins du Client. Celui-ci doit préciser 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.
 |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

PCA 02 : Test du plan de continuité d’activité

|  |
| --- |
| Le Prestataire doit tester et mettre à jour son PCA ou PCS au minimum une fois par an. Les résultats de ces tests et exercices devront être transmis au Client sur demande. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

* 1. ~~Sécurité des astreintes - ASTR~~

~~ASTR 01 : Sécurité des astreintes~~

|  |
| --- |
| ~~Dans le cas où des astreintes sont prévues, le Prestataire s'assure qu'il :~~* ~~Décrit l'architecture et les moyens techniques associés en accord avec le Client. Le Prestataire décrit en commentaire comment sont réalisées les astreintes~~
* ~~Maintient le niveau de sécurité exigé par le présent PACS~~

~~Les connexions utilisées pour les astreintes sont chiffrées et sécurisées. Préciser le dispositif en commentaire.~~~~Les connexions réalisées pour assurer l’astreinte devront figurer dans le DAT (RES 03)~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

* 1. Sécurité lors de la réversibilité - REV

REV 01 : 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 PACS liées à la conservation des traces sont toujours applicables après l’arrêt de la prestation.Le Prestataire s’engage à garantir la qualité et le maintien de la sécurité des éléments dont il a la charge (environnements, bases de données…) lors de leur restitution en fin de prestation, permettant ainsi leur pleine exploitabilité. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |

REV 02 : Destruction des données en fin de prestation

|  |
| --- |
| Le Prestataire doit disposer d’une procédure permettant la restitution et la destruction définitive des données du Client 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 le Client 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 fiscales…). |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  |  |
| Commentaire :  |

REV 03 : Phase de transfert

|  |
| --- |
| Le Prestataire devra mettre en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent soumissionnaire. |
| **Engagement Prestataire :**  |
| [ ]  Conforme  | [ ]  Non conforme  | [ ]  Non Applicable  |
| Commentaire :  |

* 1. ~~SECURITE METIER – MET~~

~~MET 01 : Sécurité des mises en production~~

|  |
| --- |
| ~~Le Prestataire est garant de la fiabilisation des mises en production dont il a la responsabilité dans le cadre de la Prestation. Le Client attend du Prestataire qu'il décrive en commentaire les moyens prévus dans le cadre de la Prestation (recette, possibilité de retour arrière...).~~~~Le Client devra être informé en cas de modification d'un environnement de production effectuée par le personnel du prestataire.~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

~~MET 02 : Règles de sécurité et d’exploitation~~

|  |
| --- |
| ~~Si le Prestataire réalise l’installation, l’exploitation ou l’administration système d’applications ou infrastructure sur le SI du Client, les moyens mis en œuvre dans le cadre des Prestations devront être conformes aux bonnes pratiques et aux règles de sécurité et d’exploitation établies par le Client. Toute exception fera l'objet d'un accord préalable écrit des équipes du Client.~~~~Le Prestataire dispose d’une politique formalisée lui permettant d’assurer l’exploitation du SI concerné.~~ |
| **~~Engagement~~****~~Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

~~MET 03 : Validité des sources d’installation des logiciels et des licences~~

|  |
| --- |
| ~~Le Prestataire doit disposer des sources d’installation des logiciels utilisés dans le cadre de la Prestation ainsi que de licences valides, lorsque ces logiciels ne sont pas mis à disposition par le Client.~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

~~MET 04 : Test de non-régression des développements~~

|  |
| --- |
| ~~Le Prestataire doit réaliser des tests de non-régression des développements réalisés.~~ |
| **~~Engagement Prestataire :~~**  |
|  |  | ~~[x]  Non Applicable~~ |
| ~~Commentaire :~~  |

1. Récapitulatif des non-conformités

*Cadre réservé aux équipes SSI SNCF.*

Les non-conformités identifiées dans le PACS sont :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref. | Nom | JUSTIFICATION DE NON-CONFORMIté | DEROGATION (Oui/non) | JUSTIFICATION DEROGATION |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Approbation

|  |  |
| --- | --- |
| **Pour le Client,** | **Pour le Prestataire,** |
| Date de signature |  | Date de signature  |  |
| Nom du signataire |  | Nom du signataire |  |
| Fonction du signataire |  | Fonction du signataire |  |
| Signature |  | Signature |  |