*Plan d’assurance sécurité*

Prestations avec hébergement de données : Éditeur XXX / Périmètre XXX

Introduction

Ce document est le Plan d’Assurance Sécurité (PAS) de la Société des Grands Projets qui est applicable entre les Parties.

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.

# Préambule

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

* Développement, intégration, paramétrage d’outils informatiques
* Hébergement de données ou de services informatiques
* Maintenance d’outils ou de matériels informatiques

Les Parties seront référées chacune par l’appellation Prestataire désignant la société [Nom de la Société] exécutant la prestation et le Client désignant la Société des Grands Projets (SGP).

# Organisation

Le Prestataire désignera un interlocuteur responsable de la sécurité du projet. Il intégrera les différentes personnes à contacter en cas d’incident rencontré.

|  |  |
| --- | --- |
| **Titre** | **Responsable** |
| **Directeur du projet** | Prénom, Nom ; Adresse e-mail |
| **Responsable de la sécurité chez le Prestataire** | Prénom, Nom ; Adresse e-mail |
| **Autre personne à contacter** | Prénom, Nom ; Adresse e-mail |

# 

# Mode opératoire de réponse

Il est demandé au Prestataire d’être conforme aux exigences applicables du PAS au démarrage de la Prestation.

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

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

Le Client pourra demander des précisions sur les engagements s’il considère que les réponses apportées par le Prestataire sur la conformité des engagements sont insuffisantes.

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

# Description de la prestation ou du service

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

# Exigence de sécurité

## Cadre juridique

Jur-01 - Loi concernant la gestion de données à caractère personnel

Le Prestataire s’engage à traiter l’ensemble des informations mises à sa disposition dans le cadre de la prestation conformément à la réglementation en vigueur.

Le Prestataire s’engage notamment à traiter ces informations conformément au RGPD - Règlement Général sur la Protection des Données.

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage à se conformer au RGPD et à notifier toutes atteintes ou violations de données à caractère personnel immédiatement après avoir pris conscience de l’incident. | | |
| Précision :  Indiquer le processus de notification au Client | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Jur-02 - Réglementation spécifique

Si, dans le cadre de la prestation contractualisée, 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.

Jur-03 - Localisation géographique des services et des données

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, dans le périmètre de la prestation, à indiquer les lieux géographiques (pays, région) dans lesquels sont localisées :   * Les services objets de la prestation * Les personnes participant à la réalisation de la prestation * Les composants techniques stockant des données Client (centres de données nominal, secours et éventuel stockage distant des sauvegardes) | | |
| Précision :  Pour les données sensibles de la SGP, le Prestataire s’engage à ce que ces données soient localisés exclusivement au sein du territoire national. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Jur-04 - Certifications du Prestataire

|  |  |  |
| --- | --- | --- |
| Si le Prestataire déclare qu’il dispose d’une certification applicable sur le périmètre de la prestation, il s’engage à fournir le justificatif de certification au Client. | | |
| Précisions :  Préciser les certifications détenues et incluses dans le périmètre de la prestation ainsi que :  - La date d’expiration de la certification  - Le périmètre définis dans le rapport de certification  Indiquer si les rapports de certifications peuvent être communiqués au Client | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Jur-05 - Répercussion des clauses sur les sous-traitants

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage, pour l’ensemble des informations manipulées et services mis en œuvre dans le cadre de la prestation, à spécifier au Client les opérateurs (sociétés et fournisseurs) amenés à intervenir en cotraitance et sous-traitance.  Le Prestataire doit répercuter les clauses du présent PAS ou équivalentes dans ses contrats de sous-traitance et de cotraitance et s’assurer de leur mise en œuvre effective.  Le Prestataire s'engage à respecter cette exigence dans le cas où un contrat de sous-traitance viendrait à être signé ultérieurement à la signature du contrat avec le Client. | | |
| Précision :  Indiquer la liste des sous-traitants amenés à intervenir sur la prestation.  Décrire comment les clauses de sécurité sont appliquées et contrôlées auprès des sous-traitants du prestataire. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Organisation de la sécurité

Org-01 - Détection, alerte et traitement des incidents de sécurité

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit disposer, sur le périmètre de la prestation, d’un processus formalisé et opérationnel de gestion des incidents de sécurité. Celui-ci devra tenir compte des phases suivantes :   * détection, * analyse * traitement, * alerte du Client | | |
| Précision :  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. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Org-02 - Gestion de crise sécurité

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation sous sa responsabilité, le Prestataire doit disposer d’un plan de gestion de crise formalisé et opérationnel tenant compte des aspects SSI.  Ce plan doit préciser au minimum :   * Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ; * La composition de la cellule de crise : fonctions et responsabilités des membres ; * Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication). | | |
| Précision : | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## 

## Ressources humaines

Hum-01 - Sensibilisation des intervenants

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit s’assurer que le personnel intervenant sur le périmètre de la prestation soit formé aux bonnes pratiques et aux bases de la sécurité au sein d’un système d’information. | | |
| Précision :  Indiquer le type et la fréquence des opérations de formation / sensibilisation | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Hum-02 - Engagement de confidentialité

|  |  |  |
| --- | --- | --- |
| Le personnel et éventuels sous-traitants du Prestataire devront avoir signé un engagement de confidentialité et de bon respect des mesures de sécurité internes. Cet engagement doit prévoir des sanctions en cas de manquements. | | |
| Précision :  Indiquer si un engagement de confidentialité est signé par le personnel intervenant dans le cadre de la prestation et si celui-ci couvre les informations des clients du Prestataire. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Gestion des actifs

Act-01 - Poste de travail

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit fournir un poste de travail qui ne servira qu’à l’usage professionnel et dont la configuration de sécurité a été renforcée. Ces postes de travail doivent notamment être équipés d’un logiciel anti-virus. | | |
| Précision :  Indiquer si un poste de travail est fourni à chacun des intervenants et préciser les mesures de sécurité implémentées sur les postes de travail | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Act-02 - Mise au rebut

|  |  |  |
| --- | --- | --- |
| Une procédure de mise en rebut des actifs est formalisée. Elle comporte notamment le processus de destruction sécurisée des données ou le processus de réaffectation du poste. | | |
| Précision :  Décrire la procédure de mise en rebut des actifs, si des actifs du Prestataire sont utilisés pour stocker des données du Client | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Gestion de l’obsolescence et des vulnérabilités

Vuln-01 - Déploiement des mises à jour de sécurité

|  |  |  |
| --- | --- | --- |
| L’ensemble des logiciels et matériels utilisés dans le cadre de la Prestation est dans une version pour laquelle l’éditeur assure le support.  De plus ces logiciels et matériels doivent être à jour en matière de correctifs de sécurité. Une procédure doit être définie et appliquée, celle-ci encadre la veille sur les correctifs de sécurité, leur analyse et leur déploiement. | | |
| Précision :  Décrire le dispositif de gestion de l’obsolescence et des mises à jour de sécurité. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Contrôle d’accès

Cac-01 - Moindre privilège

|  |  |  |
| --- | --- | --- |
| La configuration des postes de travail respecte le principe du moindre privilège. | | |
| Précision :  Décrire le dispositif de gestion de des comptes locaux d’administration | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Cac-02 - Identifiant du Prestataire

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à définir et appliquer une politique de gestion des identifiants.  Il est attendu du Prestataire :   * Que sa politique privilégie l'utilisation d’identifiants individualisés (rattachés à une personne unique) * Qu’il soit en mesure d'expliciter comment il est en mesure de relier à tout instant l'usage d'un compte non individualisé avec l'identité d'une personne   Les comptes administrateur ou de service non nécessaires doivent être désactivés.  Les comptes invités doivent être désactivés. | | |
| Précision :  Décrire les règles de gestion des identifiants et des comptes génériques et d’administration. Le cadre d’utilisation de ces comptes (finalités, cas d’usage, etc.) | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Cac-03 - Politique de mot de passe

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de mot de passe renforcée :   * Les mots de passe ont une longueur minimale * Les mots de passe comportent les quatre familles de caractères * Les authentifications utilisent le multi facteur pour les accès à distance   Les sessions doivent être doté d’un système de verrouillage automatique en cas d’inactivité. | | |
| Précision :  Décrire la politique de mot de passe implémentée sur les équipements ou applications utilisées pour stocker ou accéder à des données du Client. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Cac-04 - Administrateur

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des identifiants pour ses accès administrateurs.  Les accès administrateurs ont donc :   * Une politique de mot de passe propre au rôle d’administrateur * Une politique de renouvellement de mot de passe | | |
| Précision :  Décrire la politique de mot de passe appliquée sur le périmètre de la prestation notamment dans le cadre des accès d’administration. Préciser les éventuelles procédures d’accès distant | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Cac-05 - Traçabilité

|  |  |  |
| --- | --- | --- |
| Dans le périmètre 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 doivent contenir :   * Les accès fructueux et infructueux aux ressources * L'origine des connexions * Les informations d'horodatage   Et ce pendant une durée au minimum de 6 mois et en accord avec les exigences légales et réglementaires. | | |
| Précision :  Décrire le dispositif de traçabilité des accès aux ressources du SI Prestataire (contenu des logs, sauvegarde des logs, exploitation éventuelle des logs etc.)  Les ressources du SI Prestataire sont les applications utilisées dans le cadre de la prestation  Les accédants sont les utilisateurs et les administrateurs du Prestataire | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Cac-06 - Revue et suivi des comptes du domaine de la responsabilité du Prestataire

|  |  |  |
| --- | --- | --- |
| Une revue périodique des comptes d’accès aux ressources informatiques (serveurs, postes de travail, applications) du Prestataire utilisées dans le cadre de la prestation doit être effectuée et formalisée. | | |
| Précision :  Décrire les procédures de revue sur les ressources du SI du Prestataire (postes de travail, serveurs, équipements réseaux) : modes opératoires, périodicités, responsabilités, plan d’action en cas d’écart, etc. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Sécurité physique

Sph-01 - Accès aux locaux du Prestataire

|  |  |  |
| --- | --- | --- |
| Les locaux du Prestataire disposent d’une sécurité adéquate comprenant par exemple un système de surveillance, un contrôle des accès physique aux locaux, un système de traçabilité des accès.  Les accès sont strictement autorisés aux besoins opérationnels.  Décrire le dispositif de traçabilité des accès aux ressources du SI Prestataire (contenu des logs, sauvegarde des logs, localisation des sauvegardes, durée de conservation, exploitation éventuelle des logs etc.)  Les ressources du SI Prestataire sont les serveurs et applications utilisés dans le cadre de la prestation.  Les accédants sont les utilisateurs et les administrateurs du Prestataire | | |
| Précision :  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) | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sph-02 - Accès physique aux ressources du Prestataire

|  |  |  |
| --- | --- | --- |
| Les locaux qui hébergent les ressources techniques du Prestataire doivent être équipés d’un dispositif de contrôle d’accès individuel. Toute tentative d’accès à ces locaux doit faire l’objet d’une trace qui doit être conservée au minimum 2 mois.  Le Prestataire restreint ces accès physiques aux stricts besoins opérationnels.  Une procédure de gestion des accès physiques aux locaux techniques du Prestataire doit être formalisée. Celle-ci doit préciser au minimum les modalités de gestion des demandes et suppressions des accès ainsi qu'une revue trimestrielle. | | |
| Précision :  Décrire le dispositif de contrôle d’accès physique individuel des locaux techniques hébergeant les serveurs de données, d’infrastructure et de l’équipement réseau / télécoms (dispositif d’identification, sas d’accès, traçabilité). | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sph-03 - 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 à un système de surveillance centralisé. | | |
| Précision :  Décrire le système de protection contre les intrusions physiques (vidéosurveillance, détecteurs anti-intrusion, société de gardiennage, etc.) prévu pour les locaux techniques hébergeant les serveurs de données, d’infrastructure et de l’équipement réseau. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sph-04 - Certification des sites d'hébergement des ressources techniques

|  |  |  |
| --- | --- | --- |
| Le Prestataire indiquera le niveau de certification de ses sites hébergeant les ressources techniques ou le service liés à la prestation.  En l’absence de certification des locaux hébergeant les ressources informatiques ou le service, le Prestataire décrira les systèmes de protection et de surveillance en place contre les évènements pouvant perturber l’activité : incendie, fuite d’eau, fuite de climatisation, défaillance électrique. | | |
| Précision :  Pour les certificats, indiquer les dates d’obtention et éventuels périmètres concernés | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sph-05 - Protection contre les évènements environnementaux

|  |  |  |
| --- | --- | --- |
| Le Prestataire décrira les risques environnementaux dont font l’objet les sites hébergeant les données ou du service.  En cas de risque avéré, le prestataire précisera les mesures mises en œuvre pour couvrir ces risques (plan de prévention des risques). | | |
| Précision : | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Sécurité des données

Sdo-01 - Classification des données

|  |  |  |
| --- | --- | --- |
| Le Prestataire ne communique la classification des données utilisées dans le cadre de la Prestation qu’aux seuls intervenants ayant le « besoin d’en connaître ».  Cette communication doit être faite à l’entrée du personnel du Prestataire et à chaque modification du périmètre applicatif.  Le Prestataire demandera au Client la classification des données avant le démarrage des services et à chaque modification du périmètre applicatif. | | |
| Précision :  « Personnes ayant le Besoin d’en connaître » : i.e. personnes qui auront potentiellement accès aux données de la prestation et qui doivent être conscients de leur éventuelle sensibilité. A contrario, les intervenants du Prestataire n’accédant pas à des données sensibles utilisées dans le cadre de la Prestation ne doivent pas être informés de leur existence.  La classification des données décrit les types de données utilisées dans le cadre de la prestation ainsi que leur niveau de sensibilité (exemple de type de données : données métier SGP). Cette classification est fournie par le Client au Prestataire au démarrage de la prestation. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sdo-02 - Chiffrement des données

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage à ce que des mécanismes de chiffrements de données soient systématiquement utilisés sur tout équipements, matériels ou logiciels faisant transiter ou stockant des données confidentielles du Client (poste de travail). Ce chiffrement concerne à la fois les flux de données et le stockage de ces données. Ce chiffrement doit être effectué exclusivement par des algorithmes et protocoles robustes et à l’état de l’art (ex : SSL, TLS 1.0 et TLS 1.1 sont prohibés). | | |
| Précision :  Préciser les mécanismes de chiffrements implémentés, protocoles utilisés et périmètres applicables sur les données en transit (flux) et au repos (stockage) | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sdo-03 - Lutte contre la fuite de données

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit mettre en place des dispositifs de lutte contre la fuite de données, qu’elle soit d’origine intentionnelle ou non.  Ces dispositifs doivent couvrir les différents canaux possibles pour l’exfiltration de données :   * Réseau (ex : e-mail, internet, technologies sans fil comme le WiFi, Bluetooth) * Physique (ex : exfiltration par copie sur support amovible de type clé USB et disque dur externe ainsi que par copie sur support papier via l’impression) | | |
| Précision :  Lister les dispositifs mis en œuvre pour chaque canal de communication possible | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Sécurité dans les développements (en cas de prestation de développement informatique)

Sde-01- Formation des développeurs

|  |  |  |
| --- | --- | --- |
| En cas de prestation de développement informatique, le Prestataire doit s’assurer que le personnel mis à disposition pour réaliser ce développement soit formé sur le développement sécurisé et sur les vulnérabilités classiques. | | |
| Précision :  Fournir des exemples de formation suivi par les développeurs | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sde-02 - Utilisation d’outils d’analyse de code

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage à ce que lors d’activités de développement, il utilise des outils permettant de minimiser les erreurs introduites durant le développement ainsi que les défauts de sécurité. | | |
| Précision :  Indiquer les outils et méthodes d’analyse de code utilisés | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sde-03 - Respect des normes

|  |  |  |
| --- | --- | --- |
| Le Prestataire s’engage à respecter les normes de développement sécurisé, qu’elles soient propres au développeur, publiques ou propres au Client. | | |
| Précision :  Indiquer les normes le développement sécurisé. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Sécurité réseau

Sre-01 - Politique de gestion des flux réseau

|  |  |  |
| --- | --- | --- |
| Sur le périmètre de la prestation, le Prestataire s’engage à mettre en place une politique de gestion des flux réseau, afin de n’autoriser que les flux légitimes.  Par défaut, tous les flux qui ne sont pas explicitement autorisés doivent être interdits. | | |
| Précision :  Décrire les principes d’architecture, de cloisonnement et de filtrage des flux. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Sre-02 - Prévention contre les attaques externes

|  |  |  |
| --- | --- | --- |
| Le Prestataire mettra en œuvre des dispositifs afin de prévenir les attaques informatiques (intrusions, brute force…) sur le SI utilisé dans le cadre de la prestation. | | |
| Précision :  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.) | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Plan de continuité d’Activité

Pca-01 - Plan de continuité d’activité

|  |  |  |
| --- | --- | --- |
| Un plan de continuité d’activité doit être défini, formalisé en conformité avec le besoin Client.  Celui-ci doit préciser au minimum :   * Le périmètre du Prestataire couvert * Les scénarios de sinistre pris en compte ; * Les solutions de secours mises en œuvre ; | | |
| Précision :  Les scénarios attendus, s'ils sont applicables, peuvent notamment être :  Indisponibilité partielle ou totale des personnels du Prestataire intervenant dans le cadre de la prestation ;  Indisponibilité partielle ou totale des locaux du Prestataire hébergeant du personnel du Prestataire intervenant dans le cadre de la prestation ;  Indisponibilité des infrastructures du SI du Prestataire (postes de travail, réseau et messagerie) utilisé dans le cadre de la prestation | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Pca-02 - Test du plan de continuité d’activité

|  |  |  |
| --- | --- | --- |
| Le Prestataire doit tester et mettre à jour son plan de continuité d‘activité au minimum une fois par an. | | |
| Précision :  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.) | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Réversibilité

Rev-01 - 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 (sauf documents que le prestataire doit conserver dans le cadre de ses obligations réglementaires).  Cette procédure décrit notamment :   * La destruction des données présentes sur les postes de travail, éventuels supports numérique ou papier)   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. | | |
| Précision :  Décrire la procédure de destruction utilisée dans sur le périmètre de la prestation.  Préciser les éventuelles données que le prestataire doit conserver dans le cadre de ses obligations réglementaires. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

## Audit et contrôle de la sécurité

Ctr-01 - Contrôle de sécurité

|  |  |  |
| --- | --- | --- |
| Le Prestataire s'engage à autoriser le Client à conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés, et leurs sous-traitants.  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. | | |
| Précision :  Le Prestataire spécifie ici son accord ainsi que les modalités d'exécution et le délai de prévenance s'ils ne sont pas précisés au contrat. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

Ctr-02 - 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 un contrôle, un plan de remédiation devra être formalisé par le Prestataire au plus tard 15 jours après la livraison du rapport.  Le Prestataire devra ensuite régulariser ces écarts ou manquements par l'application du plan de remédiation dans un délai convenu en commun accord par les deux Parties.  Le Prestataire devra obligatoirement corriger ces écarts dans un temps raisonnable et pour un prix défini. | | |
| Précision :  Les retards pourront donner lieu à des pénalités financières.  Les vulnérabilités introduites durant le développement doivent être corrigées. | | |
| Engagement Prestataire : | | |
| * Conforme | * Non conforme | * Non Applicable |
| Justification en cas de critère non applicable : | | |

# Procédure d’évolution du PAS

Des modifications peuvent être apportées au PAS, dans les cas d’évolutions significatives. Par exemple et de manière non limitative :

* À la suite d’une évolution de l’analyse des risques sur le périmètre de la prestation ;
* À la suite d’une modification des modalités d'accès à l’objet de la prestation ;
* Modification de la souscription au service objet de la prestation ou modification du Contrat ;
* Modification de l’architecture technique du Prestataire impactant l’objet de la prestation, dont la modification des fonctionnalités de l’objet de la prestation ;
* À la suite d’une mise à jour qui impacte les modalités de la prestation.

La prise en compte des modifications dans le PAS est effectuée par le Client. L’application d’éventuelles nouvelles exigences de sécurité prend effet dès la signature par les deux Parties.

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

# Applicabilité du PAS

Le Plan d’Assurance Sécurité est applicable à l’ensemble des acteurs du projet, au même titre que le Plan d’Assurance Qualité et avec la même priorité.

Un acteur du projet identifiant un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement au Prestataire, qui en avertira la maîtrise d’ouvrage.

Toute modification unilatérale des présentes dispositions engage la responsabilité de la Partie qui en est à l’origine, à l’égard de l’autre Partie. En cas de non-respect du PAS, le titulaire sera redevable du paiement de pénalités. Les modalités de calcul et d’application des pénalités sont précisées au Contrat.

# Approbation

Établi à \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ le \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | Pour le Prestataire, [Fonction] : [Nom, Prénom]  Signature, Cachet de l’entreprise |
|  |  |