**ANNEXE 1 au Cahier des Clauses Particulières : Plan d’Assurance Sécurité**

# Références du prestataire :

# Objet du document

Ce document décrit l’ensemble des dispositions spécifiques que le prestataire s’engage à mettre en œuvre pour garantir le respect des exigences de sécurité de l’Université de Caen. Il définit les mesures organisationnelles, techniques, et procédurales qui seront mises en œuvre.

# Responsabilités liées au PAS

Sa rédaction relève du responsable sécurité désigné par le prestataire. Il doit être approuvé par l’université de Caen Normandie. Sa bonne exécution est de la responsabilité du prestataire en tant que maître d’œuvre.

# Evolution du PAS

Le responsable sécurité désigné par le prestataire est responsable de la rédaction du Plan d’Assurance Sécurité initial et de ses évolutions.

Une révision du Plan d’Assurance Sécurité pourra être réalisée en cas d’évolution du périmètre de l’opération ou des exigences de la maîtrise d’ouvrage, après accord de l’Université de Caen Normandie. Cette révision sera réalisée par le responsable sécurité désigné par prestataire. La version révisée du PAS sera transmise à l’Université de Caen Normandie pour validation, et diffusée à l’ensemble des acteurs pour application.

# Exigences de sécurité

## Organisation de la sécurité

En tant que maître d’œuvre, le prestataire désignera un interlocuteur responsable de la sécurité, pilotant l’ensemble de la sécurité du projet : sécurité des développements, sécurité du système d’information cible et intégration des composants sécurité.

Le prestataire décrit l’organisation de la cybersécurité mise en place dans son organisation. Il indique notamment le nom du responsable sécurité ainsi que ses coordonnées de contact.

|  |
| --- |
|  |

## Localisation des données

Le prestataire indique la liste de tous les lieux de stockage de données précise la localisation des données, (site d’hébergement principal, site(s) de secours, etc.), ainsi que la localisation des systèmes d’accès et d’administration des services. L’hébergement des données se fait dans l’union européenne.

|  |
| --- |
|  |

## Sous et co-traitance

Le prestataire devra s’assurer que ces co-traitants, sous-traitants ou fournisseurs respectent les exigences de sécurité validées conjointement avec l’université de Caen Normandie, et devra produire la documentation explicitant ce niveau de sécurité.

Le prestataire doit préciser l’ensemble des co-traitants, sous-traitants ou fournisseurs nécessaires à l’exécution de la prestation décrite.

Si des co-traitants, sous-traitants ou fournisseurs doivent intervenir directement, le prestataire indique leur rôle et précise les modalités de leur participation.

|  |
| --- |
|  |

## Protection des locaux

Le prestataire doit mettre en place des mécanismes de sécurisation de ses locaux (risques environnementaux, intrusions). Le candidat doit détailler tous les moyens mis en œuvre afin d’assurer la sécurité des locaux d’hébergement, notamment le moyens de surveillance, les dispositifs anti-intrusion , le contrôle et enregistrement des accès (gardiennage, sas, moyen d'identification, etc.), la protection physique des équipements (verrouillage des baies, etc.).

|  |
| --- |
|  |

## Protection logique

Le prestataire doit prévenir les accès logiques non autorisés au système d’information. Il décrit l’ensemble de ces mesures mises en œuvre.

|  |
| --- |
|  |

## Sécurité des réseaux

Tous les flux d’administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec,etc.), garantissant la confidentialité et l’intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

Le candidat indiquera l’ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l’intégrité des flux d’administration.

|  |
| --- |
|  |

## Sécurité des serveurs

Les serveurs doivent respecter les bonnes pratiques de sécurisation (recommandations constructeurs, guides de l’ANSSI, etc.) L’administration de ces serveurs doit se faire à partir de comptes dédiés et nominatifs.

Le prestataire décrit les mesures de sécurisation des serveurs mises en place :

|  |
| --- |
|  |

## Sécurité des postes de travail, Nomadisme et télétravail

Les postes de travail doivent disposer d’une procédure de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné. Ils doivent disposer d’un anti-virus régulièrement mis à jour. Les droits d’administrateur doivent être limités au strict minimum nécessaire.

Le stockage des données sur un espace régulièrement sauvegardé doit être favorisé. En cas de données stockées localement, ces données doivent être effacées avant ré-affectation du matériel.

En cas de nomadisme ou de télétravail, les accès à distance doivent être sécurisés via un VPN.

Le prestataire décrit sa politique de gestion des postes de travail :

|  |
| --- |
|  |

## Sécurité des développements applicatifs

Le prestataire est tenu d’assurer la sécurité des développements conformément à l’état de l’art dans chacune des technologies mises en œuvre.

Le prestataire décrira les règles qu’il applique pour garantir la sécurité de ses développement (par ex environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs, contrôle rigoureux des entrées utilisateurs, sécurisation des accès aux fonctions d’administration, principe du moindre privilège, utilisation de mots de passe dans le code interdite, mise en œuvre d’une gestion efficace des erreurs, ...)

|  |
| --- |
|  |

## Protection anti-virale

Une politique antivirale stricte devra être mise en place au niveau des serveurs dont le prestataire a la charge. La mise à jour des signatures devra être automatique et d'une fréquence élevée (30 minutes).

Le prestataire précisera la politique antivirale appliquée sur le système d’information, fournira une description des solutions anti-virus sur lesquelles se base son service de messagerie (logiciel, version) et décrira les modalités et la fréquence de mise à jour du service.

Un contrôle de non contamination des serveurs Web de production devra être effectué périodiquement. Le prestataire précisera les modalités de mise en œuvre de ce contrôle.

|  |
| --- |
|  |

## Mises à jour, correctifs de sécurité

Le prestataire s’engage à appliquer dans les plus brefs délais les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

En cas d’alerte grave (attaque virale, faille critique) annoncée par le CERTA (Centre d’Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système du donneur d’ordres (serveurs, pare-feux, routeurs ouverts vers l’extérieur).

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance hebdomadaires ou mensuelles.

Le titulaire fournit une adresse mail, un numéro de téléphone et les périodes correspondantes d’opération (H24, heures ouvrables, …) permettant à l’université de suivre le traitement d’une alerte, et décrit son processus de gestion des mises à jour et correctifs

|  |
| --- |
|  |

## Journalisation et traçabilité

Le prestataire est tenu de s’assurer qu’une journalisation des accès et des événements (système, Web…) est activée sur tous les équipements dont il a la charge. Une politique de sauvegarde de ces traces doit exister.

L’université peut être amenée à demander un extrait de ces traces, soit dans le cas d’un incident, soit à des fins de suivi de la (des) ressource(s).

Décrire la politique de conservation des traces :

|  |
| --- |
|  |

## Sauvegarde et restauration

Le prestataire effectuera des sauvegardes régulières des données de l’université. Les données sauvegardées doivent avoir un niveau de sécurité au même niveau que les données stockées sur les serveurs d’exploitation. Une au moins des sauvegardes doit être hors ligne. Les sauvegardes doivent être testées régulièrement.

Le prestataire explicite sa politique de gestion des sauvegardes :

|  |
| --- |
|  |

## Cloisonnement

Le principe de cloisonnement doit s’appliquer. Les données de l’université doivent être isolées des données des autres clients du prestataire.

Le prestataire décrit les mesures de cloisonnement mises en place ;

|  |
| --- |
|  |

## Continuité d’activité

Le prestataire doit prendre toutes les mesures nécessaires pour assurer la disponibilité du

système d’information.

Le prestataire s’engage à informer préalablement l’université de toute opération susceptible de provoquer l’indisponibilité (ou une dégradation des performances) du système.

Le prestataire s’engage à informer l’université de tout incident de sécurité impactant les données de l’université et documenter l’incident dès qu’il en a connaissance et dans un délai de 48h.

Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Le prestataire indiquera les mesures techniques, organisationnelles, procédurales qu’il s’engage à prendre pour assurer la continuité d’activité du système, ou en cas de sinistre la reprise d’activité.

Le prestataire explicite les mesures mises en place

|  |
| --- |
|  |

## Authentification et gestion des mots de passe

Les identifiants des comptes d’accès sont nominatifs. L’utilisation d’un même compte par plusieurs personnes n’est pas autorisée sauf si une contrainte le justifiant est acceptée par l’ université. Dans ce cas, le candidat présentera les mesures techniques et/ou organisationnelles pour garantir l’imputabilité.

L’utilisation de mots de passe constructeur ou par défaut est interdite.

L’utilisation de protocoles dont l’authentification est en clair est interdite.

Le prestataire doit avoir mis en place une politique de complexité des mots de passe conforme aux recommandations de l’ANSSI (longueur, complexité, protection contre les attaques par dictionnaire).

Le prestataire précise les mécanismes d’authentification mis en œuvre et détaille sa politique de sécurité des mots de passe

|  |
| --- |
|  |

## Formation et sensibilisation dans le domaine de la SSI des personnels en charge des prestations

Le prestataire doit s’assurer que le personnel en charge des prestations dispose des qualifications requises, et est sensibilisé à la Sécurité des Systèmes d’Information (SSI).

Le prestataire décrit les niveaux de qualification requis, ainsi que son plan de formation/sensibilisation en matière de SSI

|  |
| --- |
|  |

## Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien…)

Le prestataire précisera les moyens de contrôle mis en œuvre pour s’assurer du respect des exigences de sécurité de l’université par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur le système.

|  |
| --- |
|  |

## Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles) et gestion de la fin de fin des supports

Les intervenants des sociétés assurant la maintenance ou le support technique doivent être accompagnés par une personne habilitée à intervenir sur le système pendant toute la durée de leur intervention. Si un intervenant a besoin de se connecter au système, il doit utiliser un compte spécifique permettant de garantir l’imputabilité de ses actions.

Les supports de stockage de données (disques durs, bandes de sauvegardes, etc.) contenant les données de l’université de Caen ne peuvent être mis au rebut ou emportés par une société de maintenance, ou encore réutilisés à d’autres fins que celles prévues initialement. Ils doivent être conservés en lieu sûr par le titulaire, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s’assurer qu’aucune donnée ne puisse être récupérée.

Le prestataire présentera les mesures techniques et organisationnelles pour empêcher les extractions massives d’information (par exemple : extraction d’une copie de la base de données à partir d’un poste dédié à l’administration).

|  |
| --- |
|  |

## Réversibilité

En cas d'arrêt des prestations confiées au titulaire par l’université, l'ensemble des données confiées au titulaire doivent être restituées puis supprimées.

Une restitution partielle peut être demandée par l’université de Caen, en cas d’arrêt d’une partie des prestations avant la fin du marché.

À la fin de l’exécution du présent marché, le titulaire est tenu de préparer un support informatique défini par l’université de Caen contenant toutes les données de l’université gérées par le prestataire

## Résiliation

Dans le cadre d’un manquement grave par le prestataire à l’une des obligations de sécurité mises à sa charge dans le contrat, l’université pourra le mettre en demeure de réparer ce manquement. Si le manquement n’est pas réparé, l’université pourra résilier de plein droit le contrat.

## Audits de sécurité

L’université doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

Les audits pourront être réalisés par l’université, ou délégués à un tiers.