**PLAN D’ASSURANCE SECURITE**

Validation

|  |  |  |
| --- | --- | --- |
| Nom | Entité | Date |
|  |  |  |
|  |  |  |
|  |  |  |

Mise à jour

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Objet de modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table des matières

[1 CADRE D’APPLICATION DU PAS 4](#_Toc64960433)

[1.1 Objet du PAS 4](#_Toc64960434)

[1.2 Domaine d’application du PAS 4](#_Toc64960435)

[1.3 Maitrise du PAS 4](#_Toc64960436)

[1.3.1 Approbation du PAS 4](#_Toc64960437)

[1.3.2 Modification du PAS 4](#_Toc64960438)

[2 TERMES ET DEFINITIONS 5](#_Toc64960439)

[3 Documents applicables 6](#_Toc64960440)

[3.1 Documents applicables 6](#_Toc64960441)

[3.2 Règlementation applicable 6](#_Toc64960442)

[4 GOUVERNANCE DE LA SECURITE 7](#_Toc64960443)

[4.1 Organisation du TITULAIRE pour la sécurité 7](#_Toc64960444)

[4.1.1 Parties prenantes 7](#_Toc64960445)

[4.1.2 Rôles et missions 7](#_Toc64960446)

[4.2 Organisation du BENEFICIAIRE pour la sécurité 7](#_Toc64960447)

[4.2.1 Parties prenantes 7](#_Toc64960448)

[4.2.2 Rôles et missions 7](#_Toc64960449)

[4.3 Pilotage cybersécurité / COSEC 7](#_Toc64960450)

[4.4 Processus relatifs à la cybersécurité 8](#_Toc64960451)

[4.4.1 Processus de gestion des non-conformités 8](#_Toc64960452)

[4.4.2 Processus de gestion des risques sécurité 8](#_Toc64960453)

[4.4.3 Processus de gestion de crise de sécurité 8](#_Toc64960454)

[4.5 Transférabilité et réversibilité 8](#_Toc64960455)

[5 DISPOSITIONS RELATIVES A LA SECURITE 9](#_Toc64960456)

[5.1 Sensibilisation à la sécurité et à la confidentialité des données 9](#_Toc64960457)

[5.2 Gestion des identités et des accès 9](#_Toc64960458)

[5.3 Sécurité des réseaux 9](#_Toc64960459)

[5.4 Sécurité des systèmes 9](#_Toc64960460)

[5.5 Maintien en conditions de sécurité 10](#_Toc64960461)

[5.6 Hébergement et sécurité physique et environnementale 10](#_Toc64960462)

[5.7 Journalisation et surveillance 10](#_Toc64960463)

[5.8 Traitement des incidents 10](#_Toc64960464)

[6 DISPOSITIONS RELATIVES A l’AUDIT ET AU CONTROLE DE LA SECURITE 12](#_Toc64960465)

[6.1 Indicateurs sécurité 12](#_Toc64960466)

[6.2 Contrôle effectué par le BENEFICIAIRE 13](#_Toc64960467)

[6.3 Contrôle effectué par le TITULAIRE 13](#_Toc64960468)

# CADRE D’APPLICATION DU PAS

## Objet du PAS

Le BENEFICIAIRE a contracté avec le TITULAIRE dans le cadre du contrat relatif au marché [ici spécifier le nom du marché], compte tenu du savoir-faire et des compétences reconnues du TITULAIRE dans ce domaine.

Le Plan d’Assurance Sécurité (PAS) constitue une convention qui décrit les engagements de service et les dispositions d’assurance sécurité prises par le TITULAIRE pour assurer la prestation décrite dans le contrat. Ce plan est garant de la sécurité du service entre le TITULAIRE et le BENEFICIAIRE.

Il présente l’ensemble des dispositifs que le TITLAIRE s’engage à mettre en œuvre, pour obtenir un service de qualité demandé par le BENEFICIAIRE. Son but est de présenter les dispositions mises en œuvre par le TITLAIRE en termes d’organisation et de mangement de la sécurité.

L’ensemble des intervenants de la prestation doit prendre connaissance du présent PAS.

## Domaine d’application du PAS

Le PAS couvre l’ensemble des missions opérationnelles réalisées au titre du contrat :

[ici spécifier les missions ou renvoyer à un PAQ]

## Maitrise du PAS

### Approbation du PAS

Le PAS est, à l’issue de la phase d’initialisation et durant la vie du contrat :

* Approuvé en interne par le « responsable opérationnel de prestation » du TITULAIRE
* Validé en comité de pilotage par le responsable de prestation du BENEFICIAIRE

### Modification du PAS

Toute modification du PAS est traitée conjointement entre le TITULAIRE et le BENEFICIAIRE en comité de pilotage, à l’initiative de l’une des deux parties.

# TERMES ET DEFINITIONS

|  |  |
| --- | --- |
| Termes | Définition |
|  |  |
|  |  |
|  |  |

# Documents applicables

## Documents applicables

[ici spécifier les références du contrat applicable et tout autre référence utile]

## Règlementation applicable

[ici spécifier la règlementation applicable dans le domaine sécurité (ex. : RGPD)]

# GOUVERNANCE DE LA SECURITE

## Organisation du TITULAIRE pour la sécurité

### Parties prenantes

Le TITULAIRE, pour la sécurité de la mission effectuée pour le BENEFICIAIRE, est organisé comme suit :

[ici le TITULAIRE spécifie son organisation pour la sécurité de la prestation]

### Rôles et missions

[ici le TITULAIRE spécifie ses rôles et missions au titre de la sécurité de la prestation]

## Organisation du BENEFICIAIRE pour la sécurité

### Parties prenantes

Le BENEFICIAIRE, pour le suivi de la sécurité de la mission effectuée par le TITULAIRE, est organisé comme suit :

[à remplir par le BENEFICIAIRE lors de la contractualisation]

### Rôles et missions

[à remplir par le BENEFICIAIRE lors de la contractualisation]

## Pilotage cybersécurité / COSEC

[proposition de renvoi au comité de pilotage de prestation qui intègre le pilotage de sécurité]

[rempli par le BENEFICIAIRE lors de la contractualisation]

|  |  |  |
| --- | --- | --- |
| Ordre du jour | [définir les éléments du planning de suivi des actions liés à la cybersécurité] | |
| Fréquence | [définir une fréquence des COSEC] | |
| Participants | [identifier les participants côté BENEFICIAIRE] | [identifier les participants côté TITULAIRE] |
| Documents en entrée | [identifier les documents attendus au titre du suivi de la sécurité (ex : tableau de bord, support de réunion, etc.] | |
| Délai de remise des supports de comité | [indiquer le délai pour la remise des supports avant a date de réunion] | |
| Compte-Rendu de la réunion de comité | [indiquer le participant faisant la rédaction du compte-rendu du comité de sécurité et celui validant le Compte-rendu] | |

## Processus relatifs à la cybersécurité

### Processus de gestion des non-conformités

[ici le TITULAIRE spécifie son processus pour traiter les écarts constatés avec le niveau d’exigence de sécurité requis par le BENEFICIAIRE]

Les demandes de dérogation du TITULAIRE seront transmises au BENEFICIAIRE qui aura en charge de les étudier et de déterminer si elles sont ou non recevables. Celles-ci feront dans tous les cas l’objet d’un plan d’action permettant de revenir à une situation non dérogatoire.

### Processus de gestion des risques sécurité

[ici le TITULAIRE spécifie son processus de gestion des risques sécurité]

### Processus de gestion de crise de sécurité

[ici le TITULAIRE spécifie son processus de gestion de crise en y incluant :

* Son organisation
* L’application des mesures techniques
* Les conditions dans lesquelles les mesures peuvent être appliquées en tenant compte des contraintes techniques et organisation]

## Transférabilité et réversibilité

[ici le TITULAIRE spécifie les mesures techniques et organisationnelles mises en place garantissant la sécurité des données lors du transfert des prestations couvrant les domaines suivants :

* La gestion des accès et les habilitations
* Le transfert de responsabilité
* La fourniture d’informations nécessitant des mesures de protection adaptées
* La gestion de la continuité de l’activité]

# DISPOSITIONS RELATIVES A LA SECURITE

## Sensibilisation à la sécurité et à la confidentialité des données

[ici le TITULAIRE spécifie les dispositions relatives à la sensibilisation de son personnel mises en place dans le cadre de la prestation].

## Gestion des identités et des accès

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Gestion des comptes d’administrations
* Gestion des comptes individuels
* Gestion des comptes de services
* Recensement des comptes d’accès (autorisés à se connecter sur le SI)
* Application du principe du moindre privilège
* Protection contre les attaques portant sur les authentifications
* Modification des comptes par défaut

## Sécurité des réseaux

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Cloisonnement
* Filtrage
* Durcissement de configuration des équipements réseaux
* Accès distant
* Interconnexion ente le système du TITULAIRE et le système du BENEFICIAIRE]

## Sécurité des systèmes

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Sécurité des postes de travail
* Sécurité des serveurs]
* Sécurité des supports amovibles

## Maintien en conditions de sécurité

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Cartographie réseaux
* Cartographie systèmes
* Gestion des mots de passe
* Gestion de la sauvegarde et du stockage des données et des codes sources
* Protection et documentation des codes sources
* Disponibilité des données et des systèmes d’informations
* Gestion des mises à jour des logiciels et mise à jour des logiciels
* Gestion des systèmes obsolètes
* Règles de sécurité et exploitation [L’installation, l’exploitation et l’administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d’exploitation établies par la PSSIE. Toute exception fera l’objet d’un accord préalable écrit des équipes de l’acheteur]
* Mise en place d’une veille sécurité

## Hébergement et sécurité physique et environnementale

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Hébergement informatique
* Sécurité physique et environnementale

## Journalisation et surveillance

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Journalisation
* Corrélation des journaux
* Traçabilité des actions de développement

Ces procédures devront notamment porter sur la journalisation des authentifications des utilisateurs à la gestion des comptes à la gestion des droits d’accès et l’accès aux ressources du SI]

## Traitement des incidents

[ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

* Remontée d’alerte
* Enregistrement, traçabilité et gestion des incidents
* Traitement des incidents de sécurité
* Base de connaissance

# DISPOSITIONS RELATIVES A l’AUDIT ET AU CONTROLE DE LA SECURITE

## Indicateurs sécurité

[ici le TITULAIRE spécifie les indicateurs de sécurité propres à l a prestation . Les indicateurs suivants sont donnés à titre d’exemple ; à la cible, ils doivent être cohérents avec les dispositions de cybersécurité spécifiées dans le présent document.]

| Indicateurs | Formule | Cible | Fréquence |
| --- | --- | --- | --- |
| AUD-01 | Audit et contrôle  Application du plan de contrôle |  | 100 % | Mensuelle |
| MCS-01 | Patch  Nombre de serveurs dont la version OS est à jour |  | 100 % | Mensuelle |
| MCS-02 | Disponibilité et continuité #1  Application du plan de sauvegarde |  | 100 % | Mensuelle |

## Contrôle effectué par le BENEFICIAIRE

[à remplir par le BENEFICIAIRE lors de la contractualisation, en accord avec les dispositions du contrat relatives à l’audit du TITULAIRE]

Le BENEFICIAIRE se réserve le droit d’auditer l’application du PAS. A l’issue de l’audit, le rapport d'audit est soumis au TITULAIRE, incluant les mesures correctives à mettre en œuvre afin d'assurer la conformité au PAS.

Le TITULAIRE met en œuvre les mesures de sécurité correctives décidées d'un commun accord dans le délai précisé dans le plan d'actions défini en commun. Le suivi des actions de sécurité est régulièrement soumis au BENEFICIAIRE.

Si le rapport d'audit ne recommande pas explicitement les mesures à mettre en œuvre, ou si celles-ci ne peuvent raisonnablement être mises en œuvre dans de bonnes conditions, le BENEFICIAIRE proposera les actions correctives nécessaires avec l'accord du TITULAIRE.

## Contrôle effectué par le TITULAIRE

[ici le TITULAIRE spécifie décrit les dispositions relatives aux contrôles sécurité]