**Plan d’Assurance Sécurité**

**–**

**<Libellé de la prestation/service>**



**Sommaire**

[1 Avant-propos 3](#_Toc514446082)

[2 Objet et caractéristiques du plan 3](#_Toc514446083)

[3 Références 4](#_Toc514446084)

[4 Description du système et du périmètre du titulaire 4](#_Toc514446085)

[5 Rappel des exigences 5](#_Toc514446086)

[6 Organisation de la sécurité de la prestation 5](#_Toc514446087)

[6.1 Cadre organisationnel 5](#_Toc514446088)

[6.1.1 Le Comité de Contrat – Volet sécurité 5](#_Toc514446089)

[6.1.2 Le Comité de Pilotage – Volet sécurité 5](#_Toc514446090)

[6.2 Liste des participants 6](#_Toc514446091)

[6.2.1 <Le soumissionnaire> 7](#_Toc514446092)

[6.2.2 L’IRD 7](#_Toc514446093)

[7 Responsabilités liées au PAS 8](#_Toc514446094)

[8 Procédure d’évolution du PAS 8](#_Toc514446095)

[9 Applicabilité du PAS 9](#_Toc514446096)

[10 Documentations de suivi 9](#_Toc514446097)

[11 Mesures de sécurité de la prestation 10](#_Toc514446098)

[12 Matrice de couverture des exigences de sécurité 11](#_Toc514446099)

[13 Matrice de responsabilités 11](#_Toc514446100)

[14 Suivi des évolutions 12](#_Toc514446101)

# Avant-propos

Ce document « Plan d’Assurance Sécurité » est un document générique pouvant répondre à la plupart des cas de figure.

Tous les éléments explicatifs de ce modèle à retirer du document final sont en caractère rouge*.*

Tous les éléments modifiables sont en caractère bleu*.* Ces éléments sont donnés à titre d’exemples et doivent être impérativement modifiés.

Il faut tenir compte de l’environnement de l’IRD (SI administratif et/ou SI Recherche).

Le PAS doit prendre en compte la Politique de Sécurité des Systèmes d’Information de l’IRD.

Le PAS étant un document confidentiel, il ne faut pas omettre de le classifier.

**Cet avant-propos est à supprimer sur le document final.**

# Objet et caractéristiques du plan

Le Plan d’Assurance Sécurité (PAS) vise à décrire les dispositions relatives à la sécurité prises par <le soumissionnaire> pour fournir, à l’IRD, les services attendus et maintenir durablement les résultats prévus.

Une fois le titulaire nommé, le PAS est annexé au contrat. Il se substitue aux éventuelles clauses génériques de sécurité du titulaire.

Ci-dessous, le plan-type proposé est joint à l'appel d'offres comme base de rédaction du Plan d’Assurance Sécurité qui sera rédigé par le titulaire dans la phase transition.

L’objet du présent document est d’identifier les acteurs, l’organisation, les processus et activités pour gérer la sécurité dans le cadre de la réalisation du Contrat liant <le soumissionnaire> et l’IRD. Il présente les mesures physiques, organisationnelles, procédurales et techniques retenues et mises en œuvre par <le soumissionnaire> en réponse aux exigences de sécurité l’IRD.

Le Plan d’Assurance Sécurité comporte un volet organisationnel et un volet technique. Le volet organisationnel est dévolu à la gestion de la sécurité. Le volet technique identifie les mesures de sécurité répondant aux exigences relatives aux différentes phases du projet (voir chapitre 11):

* Des mesures relatives à la phase transfert (transfert de matériels ou de logiciels dans un projet d’externalisation) ou de transition,

Le soumissionnaire présente dans ce paragraphe et pour cette phase, les mesures proposées pour sécuriser, le périmètre qu’il prend en charge (récupérations de matériels et/ou de logiciels et/ou de supervision …).

Il décrit la répartition des responsabilités entre lui et l’ancien titulaire.

Il identifie ses obligations de reporting au comité de suivi sécurité.

* Des mesures relatives à la phase d’exploitation,

Le soumissionnaire présentera dans ce paragraphe les mesures mises en place pour assurer la protection du périmètre du marché et désormais, en charge du titulaire en réponse aux exigences de l’IRD.

* Des mesures relatives à la phase de réversibilité ou de fin de contrat.

Le soumissionnaire s’engage à apporter l’assistance nécessaire durant cette période de réversibilité pour faciliter le transfert des moyens de sécurité matériels et/ou logiciels et/ou de supervision, et la reprise de leur exploitation par l’IRD ou par un autre prestataire de service.

# Références

Ce paragraphe liste les documents de référence pour ce Plan d’Assurance Sécurité.

À titre d’exemple, les documents applicables peuvent être les suivants :

* Le contrat ;
* Le cahier des charges, incluant les exigences de sécurité du présent appel d’offres ;
* Le plan d’assurance qualité ;
* Etc...

# Description du système et du périmètre du titulaire

Dans ce paragraphe, le soumissionnaire présente succinctement le système faisant l’objet de l’opération d’externalisation, objet de la consultation. L’accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité. Cette description pourra éventuellement être accompagnée de schémas explicatifs commentés.

En regard du CCTP émis par l’IRD dans le cadre de cette consultation, le SI concerné se compose de …

**Eléments physiques** : énoncé des machines du périmètre

**Eléments logiques** : énoncé des logiciels et services du périmètre

**Eléments organisationnels** : énoncé des organisations et procédures du périmètre

# Rappel des exigences

Le soumissionnaire rappellera les exigences de sécurité exprimées dans le DCE ou fera référence au document les spécifiant.

# Organisation de la sécurité de la prestation

## Cadre organisationnel

### Le Comité de Contrat – Volet sécurité

Le comité de contrat (volet sécurité) a pour but de contrôler la bonne couverture du dispositif mis en place et de valider les dérogations éventuelles.

Le volet de Sécurité est abordé lors de chaque comité de Contrat. La composition de ce comité est indiquée ci-dessous en section « Liste des participants ».

### Le Comité de Pilotage – Volet sécurité

Le comité de pilotage (volet sécurité) a pour but de suivre et coordonner les actions prévues au Contrat, ainsi que les actions qui seront décidées conjointement par l’IRD et <le soumissionnaire> et placées sous la responsabilité de l’une ou de l’autre des parties prenantes.

Le volet de Sécurité est abordé lors de chaque comité de Pilotage. La composition de ce comité est indiquée ci-dessous en section « Liste des participants ».

#### Attributions

Le volet sécurité a en charge le contrôle de la prestation et de la conformité des résultats rapportés au Contrat. Il peut prendre des décisions d’ordre contractuel.

Dans ses attributions, citons :

* Le suivi et l’analyse de la bonne application de la sécurité en phase d’exploitation (rapport mensuel d’activité, tableau de bord, indicateurs de sécurité).
* La vérification de la bonne application des dispositions contractuelles. Le COCONT en mesure les écarts et étudie les propositions d’aménagements ou de révisions ainsi que les demandes de dérogation.
* Le suivi de la sécurité en phase de projets.
* Rend un avis en cas d’évolution touchant l’infrastructure
* Rend un avis en cas de régression fonctionnelle ou technique lié à l’application de la sécurité
* L’étude des propositions d’amélioration ou d’optimisation de la sécurité et la mise en œuvre des plans de progrès.
* La réponse aux questions de sécurité du COCONT et l’établissement de l’ordre du jour du prochain rendez-vous.
* S’assurer de la prise en compte globale de la sécurité, par l’IRD et <le soumissionnaire>.
* La conduite à tenir selon le résultat des audits, et des incidents ou conseils remontés par <le soumissionnaire>

#### Audit et contrôle

#### <Le soumissionnaire>

Dans le cadre de la politique générale de sécurité de son système d’information et l’amélioration de la sécurité des systèmes d’information de ses clients, <le soumissionnaire> effectue des audits de sécurité planifiés en plus des mesures de sécurité (cf. Chapitre « Mesures de sécurité »).

#### IRD

L’IRD peut, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le titulaire. Ces audits de sécurité, périodiques, pourront être réalisés par l’IRD, ou délégués à un tiers présentant des compétences en matière de sécurité.

Le contrôle est notifié à <le soumissionnaire> par courrier recommandé en définissant le périmètre de l’audit.

<Le soumissionnaire> dispose d’un délai de 10 jours ouvrés pour organiser ce contrôle.

Le décompte des jours se fait à partir du jour ouvré suivant la première présentation du courrier recommandé de la notification de visite.

Limité au périmètre strict de l’audit défini dans la notification, le contrôle s'effectue selon des modalités définies comme suit :

* Liste des modalités définies avec le client
* Visite des locaux <le soumissionnaire> liés à la prestation
* Interviews individuelles des membres des équipes projets ou d’exploitation liés à la prestation,
* Accès aux machines mises à la disposition par l’IRD
* Accès aux machines mises à la disposition par <le soumissionnaire> pour le SI de l’IRD
* ….

## Liste des participants

En tant que maître d’œuvre, <le soumissionnaire> désigne un interlocuteur responsable de la sécurité, pilotant l’ensemble de la sécurité du projet : sécurité du système d’information cible et intégration des composants sécurité. Cette fonction est assurée par le Responsable d’Exploitation Délégué.

Il pourra convier lors des volets sécurité les intervenants impliqués dans les sujets inscrits à l’ordre du jour : sécurité applicative, sécurité des serveurs, sécurité des échanges, …

Il conseille l’IRD dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

Il décrit l’implication des sous-traitants et cotraitants éventuels.

L’IRD désigne un interlocuteur responsable de la sécurité du système d’information concerné. Cet interlocuteur unique est rattaché directement à la D-DUNI de l’IRD. Cet interlocuteur est responsable de l’ensemble de la sécurité du projet pour l’IRD, tant sur les aspects sécurité du système d’information cible que sur les aspects sécurité des interfaces avec <le soumissionnaire>.

### <Le soumissionnaire>

#### Comité de Pilotage/Contrat – Volet Sécurité

| **Fonction** | **Nom** |
| --- | --- |
| **Responsable en charge de la SSI** | Prénom NOM  Adresse mail / Téléphone portable |
| **Responsable d’exploitation délégué** | Prénom NOM  Adresse mail / Téléphone portable |
| **Directeur de projet** | Prénom NOM  Adresse mail / Téléphone portable |
| **Contract Manager** | Prénom NOM  Adresse mail / Téléphone portable |
| **Autres personnes** | Prénom NOM  Adresse mail / Téléphone portable |

### L’IRD

#### Comité de Pilotage/Contrat – Volet Sécurité

|  |  |
| --- | --- |
| **Fonction** | **Nom** |
| **RSSI (Comité de Contrat)** | Prénom NOM  Adresse mail / Téléphone |
| **RSSI Adjoint - responsable sécurité opérationnelle** | Prénom NOM  Adresse mail / Téléphone |
| **Chef de projet DDUNI** | Prénom NOM  Adresse mail / Téléphone |
| **Responsable SE2I** | Prénom NOM  Adresse mail / Téléphone |
| **Responsable de production** | Prénom NOM  Adresse mail / Téléphone |
| **Autres personnes** | Prénom NOM  Adresse mail / Téléphone |

# Responsabilités liées au PAS

Le Plan d’Assurance Sécurité s’applique à :

* L’ensemble des équipes de la maîtrise d’œuvre
* Aux sous-traitants éventuels.

Sa rédaction relève du responsable sécurité désigné par <le soumissionnaire> et doit être approuvé par L’IRD ; sa bonne exécution est de la responsabilité du <le soumissionnaire> en tant que maître d’œuvre.

# Procédure d’évolution du PAS

En cas d’évolution du système, de son environnement, ou du périmètre de l’opération d’externalisation, <le soumissionnaire> vérifie si le PAS doit être modifié. La cohérence de l’ensemble des mesures pourra être analysée et réévaluée lors des réunions d’avancement (ou revues de pilotage). Si tel est le cas, il propose une modification à l’IRD. Si cette modification est acceptée, le PAS est révisé et soumis à l’IRD pour validation formelle.

Une révision du Plan d’Assurance Sécurité pourra être réalisée en cas d’évolution du périmètre de l’opération ou des exigences de l’IRD, après accord de l’IRD. Le Plan d’assurance Sécurité peut être également révisé sur demande de l’IRD.

Cette révision sera réalisée par le responsable sécurité désigné par <le soumissionnaire>. La version révisée du PAS sera transmise à l’IRD pour validation, et diffusée à l’ensemble des acteurs pour application.

Voici une liste des situations susceptibles d’entraîner une modification du PAS :

* Évolution du système d’information
  + Configuration logicielle ou matérielle ;
* Évolution de l’environnement du système d’information
  + Locaux, personnels, procédures, etc. ;
* Évolution du périmètre de l’opération
* Évolution règlementaire

# 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.

Les éventuels sous-traitants de <le soumissionnaire>, ainsi que tout personnel de <le soumissionnaire>, ou de l’IRD identifiant un non-respect du PAS, dans ses procédures et mesures, doit en référer immédiatement au <le soumissionnaire>, qui en avertira la maîtrise d’ouvrage. Un modèle type de rapport de non-respect sera annexé au PAS définitif, spécifiant la forme du rapport, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la clause de non-respect.

Si la cause du non-respect n’est pas corrigée dans un délai de <délai à estimer>, <le soumissionnaire> subira une pénalité suivant la formule : <formule à calculer>.

Un acteur du projet n’étant pas à même de remplir l’ensemble des clauses du PAS devra effectuer une demande de dérogation auprès de <le soumissionnaire>, qui négociera avec l’IRD l’ensemble des demandes de dérogation. Un modèle type de demande de dérogation sera annexé au PAS définitif, spécifiant la forme de la demande, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la demande de dérogation.

# Documentations de suivi

Le soumissionnaire recensera dans ce paragraphe l’ensemble de la documentation concernant la sécurité qu’il s’engage à fournir au titre du projet.

Les documents à fournir à l’IRD sont listés dans le tableau suivant :

|  |  |
| --- | --- |
| Nature du document : | Date de remise : |
| Plan d’Assurance Sécurité, version 1 | Remise du dossier de réponse à consultation |
| Plan d’Assurance Sécurité, version définitive | Début de phase de transfert / transition |
| Dossier de sécurité | Début de phase d’exploitation |
| Plan de secours | Début de phase d’exploitation |
| Plan de gestion des incidents | Début de phase d’exploitation |
| Comptes rendus de réunion du comité de suivi | Une semaine après chaque réunion |
| … |  |

# Mesures de sécurité de la prestation

Le soumissionnaire décrira les mesures destinées à assurer la sécurité du système cible de l’opération d’externalisation pendant les différentes phases contractuelles : phase de transfert / transition, phase d’exploitation, phase de réversibilité ou fin de contrat. Les mesures seront présentées organisées selon la structure de la PSSI de l’Etat dans le tableau suivant.

L’ensemble des mesures de sécurité à mettre en œuvre dans le cadre de cet appel d’offres sont les suivantes :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N° | Domaine PSSIE | Enoncé de la mesure | Phase de transfert | Phase d’exploitation | Phase de réversibilité |
| 001 | Sécurité des réseaux | Enoncé de la mesure 1 | X | X |  |
| 002 | Gestion des biens | Enoncé de la mesure 2 |  | X | X |

Pour mémoire les domaines de la PSSIE sont :

|  |  |
| --- | --- |
| 1. Politique, organisation, gouvernance 2. Ressources humaines 3. Gestion des biens 4. Intégration de la SSI dans le cycle de vie des systèmes d’information 5. Sécurité physique 6. Sécurité des réseaux 7. Architecture des SI | 1. Exploitation des SI 2. Sécurité du poste de travail 3. Sécurité du développement des systèmes 4. Traitement des incidents 5. Continuité d’activité 6. Conformité, audit, inspection, contrôle |

# Matrice de couverture des exigences de sécurité

Le soumissionnaire présentera les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences de cet appel d’offres. Il pourra, pour ce faire, reprendre dans un tableau à double entrée, les exigences énoncées, et lister la ou les mesure(s) répondant à chaque exigence.

Dans le cas d’une liste conséquente de mesures et/ou d’exigences, il sera possible de fournir en annexe un tableau Excel présentant cette couverture en en facilitant la lecture.

L’ensemble des mesures de sécurité présentées dans le paragraphe précédent couvent les exigences de sécurité de l’appel d’offres de la façon suivante :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Exigences de sécurité de l’IRD | | | | |
| Mesures de sécurité proposées | Enoncé de l’exigence 1 | Enoncé de l’exigence 2 | Enoncé de l’exigence 3 |  |  |
| Enoncé de la mesure 1 | X |  |  |  |  |
| Enoncé de la mesure 2 | X | X |  |  |  |
| Enoncé de la mesure 3 |  |  | X |  |  |
|  |  |  | X |  |  |
|  |  |  | X |  | X |
| … |  |  |  |  |  |

# Matrice de responsabilités

Le soumissionnaire présentera la définition des rôles et responsabilités au sein de chaque processus et activités portant sur la sécurité SI.

La matrice de responsabilité s’appliquant au périmètre du contrat est la suivante :

|  |  |  |
| --- | --- | --- |
| **Activités** | **IRD**  *Plusieurs acteurs possibles – créer autant de colonnes que d’acteurs)* | **<le soumissionnaire>**  *Plusieurs acteurs possibles – créer autant de colonnes que d’acteurs)* |
| Description de l’activité | *Rôle R, A, C, I* | *Rôle R, A, C, I* |
| … | … | … |
|  |  |  |

R = le Responsable de la mise en œuvre d'une action, d'une solution, d'une mesure, d'une procédure ....

Plusieurs "R" sont possibles, mais, dans ce cas, il faut désigner le "R" qui conduit l'opération

A = Autorité approbatrice ; sera responsable en cas de carence.

C = désigne les partenaires consultés dans leur domainee d'expertise

I = identifie les personnels informés parce qu'impactés par l'action

# Suivi des évolutions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Statut | Applicabilité | Origine et Nature évolution |
|  |  |  |  |  |