|  |  |
| --- | --- |
| Modèle de plan d’assurance sécurité (PAS)  Prestation en mode SaaS  DSI-SOC | |
| Auteur(s) : CSSI  Version : 1.1  Référence :  Diffusion : DSI | Date : 05/06/2024  Pages : 22 |
|  |  |

**Consignes pour Inria :**

**Les prestataires possédant une certification du type ISO 27001 pourront ne pas utiliser ce modèle et joindre leur propre PAS à leur réponse.**

Le plan-type proposé ci-après devra être joint à l'appel d'offres comme base de rédaction du plan d’assurance sécurité (PAS) qui sera fourni par les candidats en réponse à la consultation.

**Le contenu de ce document est à adapter par Inria pour proposer aux candidats une trame de PAS en adéquation avec les exigences de sécurité relatives au projet d’externalisation.**

Les références aux exigences de sécurité d’Inria (qui font l’objet d’un document spécifique à joindre obligatoirement à l’appel d’offres) faites dans ce document doivent obligatoirement être conservées afin que le candidat puisse s’engager à y répondre.

**Consignes pour le prestataire :**

**Les prestataires possédant une certification du type ISO 27001 pourront ne pas utiliser ce modèle et joindre leur propre PAS à leur réponse.**

Le titulaire Nom\_du\_Prestataire devra compléter chacun des chapitres de ce document.

Les demandes d’informations précisent les attendus d’Inria en tant que maître d’ouvrage. Le titulaire devra fournir les renseignements demandés.

Le découpage du document devra être respecté. Toutefois, il est possible de mettre une référence aux réponses d’un chapitre dans un autre chapitre pour faciliter la rédaction et éviter les redites.

Ce document fait référence aux exigences de sécurité d’Inria communes à toute prestation d’externalisation en mode SaaS (objet d’un document spécifique joint au marché), exigences auxquelles Nom\_du\_Prestataire s’engagera à répondre avec des mesures de sécurité adaptées qu’il décrira.

Si des réponses ont été données dans d'autres documents (réponse au CCTP, documents techniques, Plan d’Assurance Qualité), des références à celles-ci peuvent être données dans les rubriques correspondantes de ce document.

Sommaire

[1. Objet du document 5](#_Toc168496496)

[2. Documents de référence 6](#_Toc168496497)

[3. Description du système externalisé 7](#_Toc168496498)

[4. Rappel des exigences de sécurité 8](#_Toc168496499)

[5. Organisation liée à la sécurité de l’information 9](#_Toc168496500)

[5.1. Fonctions et responsabilités 9](#_Toc168496501)

[5.2. organisation en mode projet 9](#_Toc168496502)

[5.3. Séparation des tâches 10](#_Toc168496503)

[6. Responsabilités liées au PAS 11](#_Toc168496504)

[7. Procédure d’évolution du PAS 12](#_Toc168496505)

[8. Applicabilité du PAS 13](#_Toc168496506)

[9. Mesures de sécurité 14](#_Toc168496507)

[9.1. Vue d'ensemble de l'architecture 14](#_Toc168496508)

[9.2. Politiques de sécurité de l’information et gestion du risque 14](#_Toc168496509)

[9.3. Sécurité liée aux ressources humaines 15](#_Toc168496510)

[9.4. Sécurité de l'information 16](#_Toc168496511)

[9.5. Gestion des biens 16](#_Toc168496512)

[9.6. contrôle d’accès et gestion des identités 17](#_Toc168496513)

[9.7. Cryptologie 17](#_Toc168496514)

[9.8. Sécurité liée à l’exploitation 18](#_Toc168496515)

[9.9. Sécurité des opérations 19](#_Toc168496516)

[9.10. Acquisition, développement et maintenance des systèmes d’information 20](#_Toc168496517)

[10. Matrice de couverture des exigences de sécurité 21](#_Toc168496518)

[11. Documentation de suivi 22](#_Toc168496519)

# Objet du document

Ce document décrit les dispositions que Nom\_du\_Prestataire s'engage à mettre en œuvre pour répondre aux exigences de sécurité d’Inria spécifiques au projet.

Il définit en particulier l’organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d’externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

Un schéma décrivant l’architecture mise en place (machine, zones, flux, sauvegardes, accès, etc.) sera fournie en annexe.

Le prestataire doit mettre à jour les différents chapitres avec les informations adaptées à son organisation et à ses pratiques. Il sera porté une attention particulière aux paragraphes faisant référence à une mesure de sécurité. Celles-ci apparaissant entre crochet (exemple [ORG-RES-DCP-01]). Toutes les parties surlignées en jaunes doivent être remplacées par l’information attendue. Le surlignage pourra alors être supprimé

# Documents de référence

Le tableau ci-dessous indique les documents applicables et de référence liés à la sécurité.

| Nom du document | Origine | Date |
| --- | --- | --- |
| Exigences de sécurité d’Inria pour toute prestation d’externalisation | Inria | Avril 2021 |
| Politique de Sécurité de l’Information du prestataire | Nom\_du\_Prestataire |  |
| Contrat Inria/Prestataire signé | Inria |  |
| Cahier des charges (incluant les exigences de sécurité) | Inria |  |
| Guide d’hygiène informatique de l’ANSSI  <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/> | ANSSI | Sept. 2017 |
| Echelle de sensibilité des données  https://intranet.inria.fr/Inria/Directions/Direction-generale/Securite-Defense/Echelle-de-sensibilite | Inria | Mars 2020 |

# Description du système externalisé

Mise en place d'un learning management system pour Inria Academy

Le Titulaire devra assurer auprès d’Inria, tant au niveau individuel, qu’au niveau collectif (représentants de la direction, instances, groupes de travail) une fonction de conseil et de communication visant à :

* Faire la reprise du site web existant
* Organiser les inscriptions
* Organiser les formations

La nature des opérations réalisées sur les Données est : collecte, enregistrement, organisation, conservation, adaptation, consultation, utilisation, effacement.

La Finalité du Traitement est : Fournir une application et une gestion clé en main

La durée du Traitement correspondant à la durée du Marché.

Les types de Données Personnelles traitées sont : Nom, Prénom, Adresse mail, N° téléphone

# Rappel des exigences de sécurité

|  |
| --- |
| Les exigences de sécurité sont listées dans l’annexe SSI au chapitre 2 |
|  |
|  |

# Organisation liée à la sécurité de l’information

## Fonctions et responsabilités

### Sécurité des données

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [ORG-RES-SDO-01] portant sur son organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l’information.

Nom\_du\_Prestataire indiquera s’il a défini et attribué les responsabilités en matière de sécurité de l’information au personnel impliqué dans la fourniture du service et décrira le cas échéant comment il s’assure après tout changement majeur pouvant avoir un impact sur le service que l’attribution des responsabilités en matière de sécurité de l’information est toujours pertinente.

### Données à caractère personnel

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [ORG-RES-DCP-01] portant sur la protection des données personnelles.

S’il y a lieu, indiquer si une analyse d’impact relative à la protection des données à caractère personnel a bien été faite par Nom\_du\_Prestataire.

## organisation en mode projet

Décrire l’organisation proposée par Nom\_du\_Prestataire pour gérer la sécurité dans le projet d’externalisation.

Si des co-traitants, sous-traitants ou fournisseurs peuvent intervenir directement, indiquer leur rôle et préciser éventuellement les modalités de leur participation à la gestion de la sécurité du projet.

Décrire l’organisation mise en place pour assurer les relations avec le maître d’ouvrage concernant les aspects sécurité :

* Prise en compte du suivi de la sécurité (par exemple au niveau d’un comité de suivi de la sécurité ou des revues de pilotage ou d’avancement du projet) : fréquence, participants, modalités, périmètre du suivi ;
* Organisation de la maîtrise d’ouvrage : responsable sécurité, rôle et moyens ; intervenants techniques ;
* Organisation du prestataire : responsable sécurité, rôle et moyens ;
* Responsables techniques, implication des co-traitants et sous-traitants éventuels ;
* Diffusion du Plan d’assurance sécurité et des documents de suivi ;
* Audits, contrôles réalisés par la maîtrise d’ouvrage ou à la demande de celle-ci : modalités, périmètre, exploitation des résultats.

### Organisation de la maîtrise d’œuvre

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria **[ORG-PRO-MOE-01]** portant sur son organisation de la maîtrise d’œuvre.

### Organisation de la maîtrise d’ouvrage

Nom\_du\_Prestataire a pris connaissance de l’organisation de la maîtrise d’ouvrage d’Inria au travers de l’exigence de sécurité d’Inria **[ORG-PRO-MOA-01]** et s’engage à collaborer avec Inria conformément à celle-ci.

## Séparation des tâches

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité **d’Inria [ORG-SPT-SPT-01]** portant sur les risques associés à des cumuls de responsabilités ou de tâches.

S’il y a lieu, décrire les mesures de réduction de ces risques mises en œuvre.

# Responsabilités liées au PAS

Nom\_du\_Prestataire, au travers de son responsable de la sécurité désigné, est responsable de la rédaction, de l’évolution et de l’application du plan d’assurance sécurité (PAS) tout au long du contrat.

Le PAS s’applique à l’ensemble des équipes de la maîtrise d’œuvre (et aux sous-traitants éventuels). Il doit être approuvé par la DSI, qui porte le projet et la maîtrise d’ouvrage d’Inria. Sa bonne exécution est de la responsabilité de Nom\_du\_Prestataire en tant que maître d’œuvre.

La cohérence de l’ensemble des mesures pourra être analysée et réévaluée lors des réunions d’avancement (ou revues de pilotage).

# Procédure d’évolution du PAS

Une révision du PAS pourra être réalisée en cas d’évolution du périmètre des opérations ou des exigences de la maîtrise d’ouvrage d’Inria et ce, après accord avec la maîtrise d’œuvre.

Cette révision, qui devra faire l’objet d’un avenant au contrat, sera réalisée par le responsable sécurité désignée par Nom\_du\_Prestataire. La version révisée du PAS sera transmise à la maîtrise d’ouvrage d’Inria pour validation, et diffusée à l’ensemble des intervenants du projet pour application.

# Applicabilité du PAS

Le PAS est applicable à l’ensemble des acteurs du projet, au même titre que le PAQ[[1]](#footnote-1) et avec la même priorité. Un acteur du projet identifiant un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement à Nom\_du\_Prestataire, qui en avertira la maîtrise d’ouvrage d'Inria.

Si la cause du non-respect n’est pas corrigée dans un délai de délai à estimer, Nom\_du\_Prestataire subira une pénalité suivant la formule 0: 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 Nom\_du\_Prestataire, qui négociera avec la maîtrise d’ouvrage d'Inria l’ensemble des demandes de dérogations.

# Mesures de sécurité

## Vue d'ensemble de l'architecture

### Accès à la solution par les utilisateurs Inria

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-ARC-ASU-01] portant sur les accès sécurisés à la solution.

Nom\_du\_Prestataire indiquera la méthode d’accès à la solution qu’il compte mettre en place, par exemple :

* Accès direct depuis un navigateur à l’aide de connexions type HTTPS. Dans ce cas, Nom\_du\_Prestataire indiquera s’il compte limiter les plages d’adresse IP pouvant accéder à la solution.
* Accès grâce à un VPN qu’il met en œuvre pour les besoins d’Inria (préciser quel type de VPN)
* Accès via un portail dédié de type reverse-proxy. Il précisera où se trouve ce portail, si ce portail est internalisé chez Inria ou au contraire hébergé ailleurs.
* S’il y a lieu, Nom\_du\_Prestataire indiquera si un tunnel chiffré type IPSec sera mis en œuvre entre les infrastructures d’Inria et les siennes

Indiquer comment se feront l’authentification et l’identification des utilisateurs Inria. Par exemple :

* + Compte locaux gérés dans le service. Préciser qui crée et gère ces comptes.
  + Mise en œuvre d’une solution SSO (SAMLv2, OpenId, etc.). Nom\_du\_Prestataire indiquera comment se fait l’habilitation des utilisateurs (association des utilisateurs à un profil défini dans le service, utilisation d’attributs, etc.).

Nom\_du\_Prestataire précisera les mesures de protection qu’il compte mettre en place contre les tentatives d’accès illégitimes en se basant si besoin sur les exemples fournis dans l’exigence de sécurité d’Inria [MES-ARC-ASU-01] .

## Politiques de sécurité de l’information et gestion du risque

### Principes

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-PSI-PRI-01] portant sur l’opération de la prestation à l’état de l’art et l’application du guide d’hygiène informatique de l’ANSSI[[2]](#footnote-2) au système d’information du service fourni.

### Charte informatique du prestataire

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-PSI-CHA-01] portant sur sa charte informatique.

Dans le cadre du télétravail de ses collaborateurs, Nom\_du\_Prestataire indiquera quelles règles de protection sont mises en œuvre sur les matériels hors bureaux. Nom\_du\_Prestataire décrira comment il compte s’assurer que le niveau de sécurité de la prestation liée au télétravail n’est pas dégradé (utilisation systématique d’un VPN, clés RSA, vérifications régulières, etc.).

Nom\_du\_Prestataire indiquera s’il dispose d’une charte informatique spécifique pour les administrateurs informatiques.

Si possible il joindra sa charte informatique à sa réponse.

### Politique de sécurité de l’information

La politique de sécurité de l’information doit identifier les engagements de Nom\_du\_Prestataire quant au respect de la législation et réglementation nationale en vigueur (règlement général sur la protection des données - RGPD[[3]](#footnote-3), loi 78-17 du 6 janvier 1978 modifiée, etc.) selon la nature des informations qui pourraient être confiées par Inria à Nom\_du\_Prestataire.

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-PSI-PSI-01] portant sur sa politique de sécurité de l’information.

Il indiquera s’il révise régulièrement sa politique de sécurité de l’information et à quelles occasions (annuellement, à chaque changement majeur pouvant avoir un impact sur le service, etc.).

### Appréciation des risques de sécurité

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-PSI-RIS-01] portant sur son appréciation des risques de sécurité pesant sur le périmètre du service fourni.

Il précisera s’il révise régulièrement cette appréciation des risques et à quelles occasions (annuellement, à chaque changement majeur pouvant avoir un impact sur le service, etc.).

## Sécurité liée aux ressources humaines

### Sensibilisation, qualification et formations en matière de sécurité de l’information

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-SRH-SEN-01] portant sur la sensibilisation ou formation à la sécurité de ses salariés, contractants et utilisateurs tiers.

Il précisera la méthode de formation, le public concerné et la fréquence d’exécution de cette formation.

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-SRH-SEL-01] portant sur la vérification des informations de son personnel pour toute prise de poste.

## Sécurité de l'information

### Protection des données

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-SEC-PRO-01] portant sur la protection des données du projet.

### Suppression des données d’Inria

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-SEC-SUP-01] portant sur la suppression des données d’Inria en fin de contrat ou en cas de rupture anticipée ou encore à la demande d’Inria.

Décrire le procédé utilisé et préciser les délais applicables pour l’effacement de l’intégralité des informations d’Inria.

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-SEC-CLA-01] portant sur sa conformité à l’échelle de sensibilité des données d’Inria et précisera de quelle manière il procède au marquage de l’information.

Il décrira comment il compte organiser les données liées au projet (utilisation d’une arborescence spécifique par exemple) et comment il donnera accès à l’information classifiée.

## Gestion des biens

### Inventaire des biens

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-BIE-INV-01] portant sur l’inventaire de ses biens, en lien avec le projet ou non.

### Mise au rebut d’un matériel

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-BIE-REB-01] portant sur sa procédure pour l’effacement sécurisé des données stockées ou leur destruction lors de la mise au rebus d’un matériel.

S’il y a lieu, Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-BIE-AMO-01] portant sur sa procédure de gestion des supports amovibles.

### Recyclage sécurisé du matériel

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-BIE-REC-01] portant sur l’effacement sécurisé des supports de données en cas de recyclage.

Nom\_du\_Prestataire précisera le procédé utilisé pour cette opération.

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-BIE-REB-01] portant sur sa procédure pour l’effacement sécurisé des données stockées ou leur destruction lors de la mise au rebus d’un matériel.

## contrôle d’accès et gestion des identités

Sauf mention explicite, ce chapitre concerne le contrôle d’accès et la gestion des identités des utilisateurs :

* Placés sous la responsabilité de Nom\_du\_Prestataire (ses employés et éventuellement des tiers participant à la fourniture du service) ;
* Placés sous la responsabilité d’Inria, mais pour lesquels Nom\_du\_Prestataire met en œuvre les moyens de contrôle d’accès (en fournissant notamment à Inria une interface de gestion des comptes et des droits d’accès).

Les utilisateurs pour lesquels Inria met directement en œuvre les moyens de contrôle d’accès et de gestion des identités sont hors du champ d’application de ce document.

### Enregistrement et suppression des utilisateurs

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-ACC-ESU-01] portant sur sa procédure d’enregistrement et de suppression des utilisateurs dans l’outil de gestion des droits d’accès.

Nom\_du\_Prestataire précisera notamment si la suppression d’un utilisateur entraîne la suppression de tous ses accès aux ressources du système d’information.

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-ACC-POL-01] portant sur sa politique de gestion des identités et des contrôles d’accès.

Il précisera avec quelle fréquence cette politique est revue.

### Gestion des droits d’accès

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-ACC-GES-01] portant sur sa gestion des droits d’accès.

Il précisera en particulier si les comptes administrateurs sont nominatifs.

## Cryptologie

### Hachage des mots de passe

S’il y a lieu, Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-CRY-MDP-01] sur le stockage de mots de passe en base, et mentionnera la fonction de hachage utilisée.

Indiquer si les mots de passe sont salés avant d’être hachés.

Nom\_du\_Prestataire indiquera si les données stockées sont chiffrées, le cas échéant il mentionnera la solution de chiffrement utilisée.

### Chiffrement des flux

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-CRY-FLU-01] portant sur la sécurisation des flux et décrira le mécanisme de chiffrement mis en place.

## Sécurité liée à l’exploitation

### Procédures d’exploitation documentées

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-PRO-01] portant sur ses procédures d’exploitation.

### Gestion des changements

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-CHG-01] portant sur ses procédures de gestion des changements apportés aux systèmes en production.

### Séparation des environnements

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-SEP-01] portant sur la séparation des environnements de production des autres environnements.

### Mesures contre les codes malveillants

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-MAL-01] portant sur ses mesures de détection, de prévention et de restauration pour se protéger des codes malveillants.

### Sauvegarde des informations

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-SAV-01] portant sur sa politique de sauvegarde mise en place : objet de la sauvegarde, sa fréquence, les tests, l’éventualité du chiffrement, etc.

Il précisera notamment :

* Si des copies de sauvegarde des informations, des logiciels et de leurs configurations sont effectuées quotidiennement ;
* Si les sauvegardes font l’objet d’une traçabilité revue de façon hebdomadaire ;
* Si les sauvegardes sont soumises à un essai de restauration et selon quel cycle ;
* Où sont localisées les sauvegardes ;
* Lorsque les sauvegardes sont traitées par un sous-traitant ou sont externalisées, si elles sont chiffrées ;
* S’il y a lieu, quelle est la performance du système de sauvegarde, en termes de RTO et RPO[[4]](#footnote-4).

### Journalisation des événements

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-JOU-01] portant sur la journalisation des événements.

Il décrira comment sont collectés et tenus à jour les journaux d’événements enregistrant les activités des utilisateurs (tant au niveau système qu’applicatifs et composants logiciels tels bases de données), les exceptions, les défaillances et les événements liés à la sécurité de l’information.

Nom\_du\_Prestataire indiquera comment sont collectés et tenus à jour les journaux d’événements enregistrant les activités des administrateurs système et des opérateurs système dans des mécanismes de journalisation dédiés.

Il précisera comment et combien de temps sont conservés les journaux. Il indiquera également si Inria a accès à ces journaux et par quel moyen.

### Protection de l’information journalisée

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-PJO-01] portant sur la protection de l’information journalisée.

Nom\_du\_Prestataire précisera :

* S’il a estimé l’espace de stockage nécessaire à la conservation locale des journaux lors du dimensionnement des équipements ;
* Si les journaux de l’ensemble des équipements du système d’information sont transférés de manière sécurisée sur un ou plusieurs serveurs centraux dédiés et stockés de manière sécurisée sur une machine différente de celle qui les a générés ;
* Si les processus de journalisation et de collecte sont exécutés par des comptes disposant de peu de privilèges ;
* Si l’accès aux journaux est limité à un nombre restreint de comptes (seul ceux ayant besoin de l’information).

### Synchronisation des horloges

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-EXP-HOR-01] portant sur la synchronisation des horloges des équipements et l’horodatage de tous les journaux.

## Sécurité des opérations

### Politique de sécurité et procédures de traitement et d’échange d’information

Nom\_du\_Prestataire s’engage à répondre à l’exigence de sécurité d’Inria [MES-OPE-PRO-01] portant sur ses politiques, procédures et mécanismes de sécurité pour protéger toutes les opérations qui s’effectuent sur son système d’information.

### Politique de cloisonnement

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-OPE-CLO-01] portant sur sa politique de cloisonnement.

### Mesures sur les réseaux et les systèmes

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-OPE-RES-01] concernant les mesures de sécurité mises en place sur les réseaux et les systèmes.

Dans le cas où des services, protocoles ou ports réputés non sûrs doivent être néanmoins utilisés, Nom\_du\_Prestataire décrira les mesures compensatrices qu’il a mises en place dans une logique de défense en profondeur.

Nom\_du\_Prestataire indiquera si la documentation et les schémas d'architecture système et réseau identifient clairement les environnements sensibles et les flux de données pour lesquels la conformité légale, statutaire ou réglementaire est à considérer.

Nom\_du\_Prestataire listera les éventuelles mesures mises en œuvre pour appliquer des techniques de défense en profondeur telles que listées dans l’exigence de sécurité d’Inria [MES-OPE-RES-01].

### Sécurité des services

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-OPE-SER-01] portant sur la sécurité des services fournis.

## Acquisition, développement et maintenance des systèmes d’information

### Politique de développement sécurisé

Nom\_du\_Prestataire décrira comment il s’engage à répondre à l’exigence de sécurité d’Inria [MES-ADM-POL-01] portant sur son cycle et ses pratiques de développement.

# Matrice de couverture des exigences de sécurité

Nom\_du\_Prestataire présentera les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences de sécurité d’Inria décrite dans le document d’exigences de sécurité d’Inria ainsi qu’au chapitre 4 de ce document. Il pourra pour ce faire reprendre dans un tableau les exigences énoncées, et lister la ou les mesure(s) répondant à chaque exigence.

# Documentation de suivi

Nom\_du\_Prestataire recensera dans ce paragraphe l’ensemble de la documentation concernant la sécurité qu’il s’engage à fournir au titre du projet. Ces documents pourront être les suivants :

| 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 |
| 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 |

1. Plan d’Assurance Qualité [↑](#footnote-ref-1)
2. Lien : <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/> [↑](#footnote-ref-2)
3. Lien : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees> [↑](#footnote-ref-3)
4. RTO (*Recovery Time Objective*) et RPO (*Recovery Point Objective*) [↑](#footnote-ref-4)