Plan d’assurance Sécurité

(PAS)

**POUR LE LOT 1 et LOT 2**

SOMMAIRE

[1.0 OBJECTIF DU DOCUMENT 4](#_Toc152586010)

[2.0 MAITRISE DU DOCUMENT 5](#_Toc152586011)

[2.1 Rédaction 5](#_Toc152586012)

[2.2 Validation 5](#_Toc152586013)

[2.3 Mise à jour 5](#_Toc152586014)

[2.4 Diffusion 5](#_Toc152586015)

[3.0 GESTION DU PLAN D’ASSURANCE SECURITE 6](#_Toc152586016)

[3.1 Procédure de mise à jour 6](#_Toc152586017)

[3.2 Procédure de validation 6](#_Toc152586018)

[3.3 Procédure de diffusion 6](#_Toc152586019)

[3.4 Procédure de dérogation au PAS 6](#_Toc152586020)

[3.5 Procédure de contrôle du respect du PAS 6](#_Toc152586021)

[3.6 Procédure en cas de non-respect du PAS 6](#_Toc152586022)

[3.7 Documents applicables et documents de référence 6](#_Toc152586023)

[3.7.1 Documents applicables 6](#_Toc152586024)

[3.7.2 Documents de référence 6](#_Toc152586025)

[3.8 Points de Contact 6](#_Toc152586026)

[3.8.1 CNRS 6](#_Toc152586027)

[3.8.2 Titulaire 7](#_Toc152586028)

[4.0 SITES 8](#_Toc152586029)

[4.1 Sites du CNRS 8](#_Toc152586030)

[4.2 Sites du Titulaire 8](#_Toc152586031)

[5.0 ORGANISATION ET GOUVERNANCE 9](#_Toc152586032)

[5.1 Organisation du CNRS 9](#_Toc152586033)

[5.1.1 Schéma d’organisation SSI 9](#_Toc152586034)

[5.1.2 Les missions du CNRS en matière de SSI 9](#_Toc152586035)

[5.2 Organisation du Titulaire 9](#_Toc152586036)

[5.2.1 Schéma d’organisation SSI 9](#_Toc152586037)

[5.3 Gestion des dérogations 9](#_Toc152586038)

[6.0 MESURES DE PROTECTION 10](#_Toc152586039)

[6.1 Organisation de la sécurité du SI 10](#_Toc152586040)

[6.2 Sécurité physique et environnementale 10](#_Toc152586041)

[6.3 Contrôle des accès logiques et privilégiés 11](#_Toc152586042)

[6.3.1 Procédure d’habilitation interne 11](#_Toc152586043)

[6.3.2 Politique de gestion des identifiants et mots de passe 11](#_Toc152586044)

[6.4 Protection des données 11](#_Toc152586045)

[6.5 Intégration de la sécurité dans les projets 11](#_Toc152586046)

[6.6 Formation et sensibilisation des intervenants 12](#_Toc152586047)

[6.7 Gestion des incidents 12](#_Toc152586048)

[6.8 Exploitation 12](#_Toc152586049)

[6.9 Contrôle et conformité 13](#_Toc152586050)

[6.9.1 Gestion des licences 13](#_Toc152586051)

[6.9.2 Protection des données personnelles 13](#_Toc152586052)

[7.0 DESCRIPTION DES PROCESSUS APPLICABLES 14](#_Toc152586053)

[7.1 Mesures applicables 14](#_Toc152586054)

1. OBJECTIF DU DOCUMENT

Ce document constitue le Plan d’Assurance Sécurité (PAS) de l’accord-cadre relatif aux PRESTATIONS DE SERVICES DE CONTRÔLE LÉGAL ET DE CERTIFICATION DES COMPTES INDIVIDUELS ET CONSOLIDÉS DU CNRS.

Il décrit l’organisation, les acteurs, les processus, mesures et procédures mis en œuvre par le Titulaire pour assurer un niveau de sécurité en adéquation avec les mesures applicables de la PSSI du CNRS.

|  |
| --- |
| **Remarques :**  **→** Dans le présent document, les rubriques où il est fait la mention suivante : « *A initialiser par le candidat »* seront à remplir par le candidat dans le cadre de son offre. **Il est attendu de la part du candidat un début de réponse**.  *→* Dans le présent document, les rubriques où il est fait la mention suivante : « *A compléter par le candidat / A compléter par le candidat dans le cadre de son offre »* seront à remplir par le candidat dans le cadre de son offre. **Il est attendu de la part du candidat une réponse exhaustive**.  **→** Dans le présent document, les rubriques où il est fait la mention suivante : **«***A compléter par le titulaire à l’initialisation »* seront à remplir par le titulaire à compter du démarrage des prestations du présent accord-cadre. **Ainsi, au stade de son offre, le candidat n’a pas à remplir ces rubriques.** |

1. MAITRISE DU DOCUMENT
   1. Rédaction

|  |  |  |  |
| --- | --- | --- | --- |
| Rédacteur | Titre | Origine | Date de Production |
|  |  |  | -- / -- / ---- |
|  |  |  | -- / -- / ---- |

* 1. Validation

|  |  |  |  |
| --- | --- | --- | --- |
| Validation Titulaire | Titre | Visa | Validé le |
|  |  |  | -- / -- / ---- |
|  |  |  | -- / -- / ---- |

|  |  |  |  |
| --- | --- | --- | --- |
| Validation CNRS | Titre | Visa | Validé le |
|  |  |  | -- / -- / ---- |
|  |  |  | -- / -- / ---- |

* 1. Mise à jour

|  |  |  |  |
| --- | --- | --- | --- |
| Rédacteur | Chapitre / Motif | Version | Date de Production |
|  |  |  | -- / -- / ---- |
|  |  |  | -- / -- / ---- |

* 1. Diffusion

Pour le CNRS, le CNRS diffuse le PAS aux destinataires suivants :

|  |  |
| --- | --- |
| Nom | Titre |
|  |  |
|  |  |

Pour le Titulaire, le Titulaire diffuse le PAS aux destinataires suivants :

|  |  |
| --- | --- |
| Nom | Titre |
|  |  |
|  |  |

1. GESTION DU PLAN D’ASSURANCE SECURITE
   1. Procédure de mise à jour

*A initialiser par le candidat*

* 1. Procédure de validation

*A initialiser par le candidat*

* 1. Procédure de diffusion

*A initialiser par le candidat*

* 1. Procédure de dérogation au PAS

*A initialiser par le candidat*

* 1. Procédure de contrôle du respect du PAS

*A initialiser par le candidat*

* 1. Procédure en cas de non-respect du PAS

*A initialiser par le candidat*

* 1. Documents applicables et documents de référence
     1. Documents applicables

*PSSI du CNRS : Organisation pour les Délégations Régionales*

*Le Délégué Régional est le responsable de la sécurité des systèmes d’information pour son unité, il nomme un Chargé de la SSI (CSSI) pour la mise en œuvre de cette PSSI dans son unité. Par défaut, le RSSI de la DR est le CSSI pour son unité.*

* + 1. Documents de référence

*Autres documents de référence dans le référentiel du candidat*

* 1. Points de Contact
     1. CNRS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priorité | Nom | Fonction | Téléphone | Mobile | E-mail | Plage de Service |
| #1 | Fersing Christophe | RSSI DR16 |  |  | [christophe.fersing@cnrs.fr](mailto:Christophe.fersing@cnrs.fr) |  |

* + 1. Titulaire

*A compléter par le titulaire à l’initialisation*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priorité | Nom | Fonction | Téléphone | Mobile | E-mail | Plage de Service |
| #1 |  | RSSI/Contact SSI contrat |  |  |  |  |
| #2 |  | DPO |  |  |  |  |
| #3 |  |  |  |  |  |  |
| #4 |  |  |  |  |  |  |
| #5 |  |  |  |  |  |  |

1. SITES
   1. Sites du CNRS

Se reporter à l’article III du CCTP.

* 1. Sites du Titulaire

*A compléter par le candidat*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Site | Adresse physique | Adresse postale | Nom du point de contact | Téléphone du point de contact | E-mail du point de contact | Prestations réalisées sur le site |
| #1 |  |  |  |  |  |  |
| #2 |  |  |  |  |  |  |
| #3 |  |  |  |  |  |  |
| #4 |  |  |  |  |  |  |
| #5 |  |  |  |  |  |  |

1. ORGANISATION ET GOUVERNANCE
   1. Organisation du CNRS
      1. Schéma d’organisation SSI

L’autorité responsable de la SSI (AQSSI) est le Président du CNRS. Le Directeur Général-Délégué aux Ressources est chargé de l’organisation et du pilotage de la sécurité des SI, assisté d’un comité de pilotage de la sécurité des systèmes d’information et d’un RSSI CNRS (RSSIC).

Le RSSI DR est nommé, dans chaque délégation régionale, après avis du RSSIC. Le RSSI DR anime le réseau des chargés de sécurité des systèmes d’information (CSSI) des unités suivies par sa délégation.

Le RSSI DR s’entoure d’experts SSI appartenant à des unités de recherche, pour former une coordination régionale de la SSI (CRSSI) apte à apporter un support SSI aux Laboratoires et entités de sa DR.

Il gère les alertes et incidents, il signale tout incident de sécurité à la chaine fonctionnelle. Il applique les mesures de sécurité (mises à jour des OS, etc.) sur les infrastructures et dans les projets de SI (analyse de risque, etc.) de la délégation.

* + 1. Les missions du CNRS en matière de SSI

*Ces éléments seront complétés par le CNRS au démarrage de la prestation.*

* 1. Organisation du Titulaire
     1. Schéma d’organisation SSI

*A compléter par le candidat.*

* 1. Gestion des dérogations

*A compléter par le Titulaire à l’initialisation*

1. MESURES DE PROTECTION

*Le candidat doit, en complément des thématiques listées ci-dessous, préciser toutes les mesures de sécurité dont il jugera qu’elles sont de nature à réduire les risques identifiés.*

* 1. Organisation de la sécurité du SI

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes :*

* *existence d’une Politique de Sécurité du Système d’Information ;*
* *formalisation des responsabilités SSI chez le Titulaire ;*
* *politique de sécurité de l’information pour les relations avec les tiers ;*
* *intégration de la sécurité dans les contrats des tiers.*
  1. Sécurité physique et environnementale

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes (concernant les sites d’exécution des prestations) :*

* *définition des zones de sécurité ;*
* *contrôle d'accès physique des zones sensibles ;*
* *contrôle des zones de livraison ;*
* *protection des bureaux, des salles et autres locaux ;*
* *protection contre les défaillances des moyens généraux – onduleur et groupe électrogène ;*
* *sécurité du câblage – séparation des courants forts et des courants faibles.*
  1. Contrôle des accès logiques et privilégiés
     1. Procédure d’habilitation interne

*A compléter par le candidat*

* + 1. Politique de gestion des identifiants et mots de passe

*A compléter par le candidat*

* 1. Protection des données

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes :*

* *formalisation de règles d’utilisation des actifs ;*
* *politique de classification de l’information ;*
* *mise en œuvre de la politique de classification de l’information ;*
* *marquage de l’information ;*
* *formalisation de règles de manipulation des actifs en rapport avec leur classification ;*
* *anonymisation des données sur les environnements de formation et hors production à l’exception de l’environnement de recette et de la copie à l’usage de l’OMES-DRH ;*
* *politique et procédures d'échange de données – avec le CNRS ;*
* *politique et procédures d'échange de données – avec les tiers ;*
* *protocoles d'accord relatifs aux échanges de données – avec le CNRS ;*
* *protocoles d'accord relatifs aux échanges de données – avec les tiers ;*
* *sécurité des échanges par messagerie électronique ;*
* *autorisation avant déplacement hors-site du matériel ;*
* *sécurité des équipements hors-site ;*
* *transport des supports de stockage physiques ;*
* *gestion des supports de stockage amovibles ;*
* *fin de vie des supports de stockage ;*
* *recyclage et fin de vie sécurisée du matériel ;*
* *anonymisation des données.*
  1. Intégration de la sécurité dans les prestations

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes :*

* *intégration de la sécurité dans la gestion des prestations :*
  + *pour l’exécution des Prestations ;*
  + *pour la gestion des échanges ;*
  + *pour la fin du contrat de la prestation ;*
* *spécification et analyse des exigences de sécurité dans les projets/prestations.*
  1. Formation et sensibilisation des intervenants

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes :*

* *sélection des collaborateurs ;*
* *clauses SSI dans les contrats de travail ;*
* *responsabilités du management dans l'application de la SSI ;*
* *politique du bureau et de l’écran propre ;*
* *procédure disciplinaire ;*
* *sensibilisation et formation SSI des collaborateurs ;*
* *sensibilisation et formation SSI des sous-traitants du titulaire ;*
* *gestion du télétravail (si applicable) ;*
* *politique relative aux terminaux mobiles (si applicable) ;*
* *clauses de confidentialité - collaborateurs du Titulaire ;*
* *clauses de confidentialité - sous-traitants du Titulaire.*
  1. Gestion des incidents

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes :*

* *journalisation des événements ;*
* *protection des journaux et des traces ;*
* *journaux d’administration et d’exploitation ;*
* *synchronisation horaire des équipements ;*
* *chaîne de signalement des incidents de sécurité ;*
* *chaîne de signalement des failles de sécurité ;*
* *analyse et prise de décision sur les incidents de sécurité ;*
* *dispositif de réponse aux incidents de sécurité ;*
* *dispositif de capitalisation sur les incidents de sécurité ;*
* *procédures de collecte de preuve.*
  1. Exploitation

***L’offre du Titulaire détaille particulièrement les moyens, procédures et méthodes mises en œuvre pour la coordination et la planification des activités de maintenance avec les fournisseurs en cohérence avec le planning d'exploitation et d'utilisation et avec les dispositifs consacrés à maintenir la confidentialité des données***

*A compléter par le candidat dans le cadre de son offre, en abordant notamment les thématiques suivantes :*

* *contrats de maintenance pour les équipements ;*
* *documentation des procédures d’exploitation ;*
* *contrôle de l’utilisation des programmes utilitaires à privilèges ;*
* *gestion des clés cryptographiques ;*
* *utilisation de protocoles sécurisés dans le cadre des actions d’exploitation ;*
* *protection contre les logiciels malveillants ;*
* *segmentation des réseaux ;*
* *protection des réseaux ;*
* *protection des services applicatifs sur les réseaux publics, notamment contre les dénis de service, distribués ou non ;*
* *protection des applications sur les réseaux publics ;*
* *gestion des environnements et équipements mutualisés ;*
* *politique d’application des correctifs de sécurité.*
  1. Contrôle et conformité
     1. Gestion des licences

*A compléter par le candidat*

* + 1. Protection des données personnelles

*A compléter par le candidat*