MINISTÈRE
CHARGÉ
DES TRANSPORTS
Liberté
Égalité
Fraternité

Direction interdépartementale

des routes Centre-Est

Plan d'Assurance Sécurité

Cadre de réponse type

Marché de maintenance des réseaux de transmission des PC de la DIR Centre-Est

Table des matières

Plan d'Assurance Sécurité....1
1 Objet du PAS....3
2 Documents de référence....3
3 Rappel des exigences....3
4 Organisation et gouvernance....3
5 Responsabilités liées au PAS....5
6 Procédure d'évolution du PAS....6
7 Applicabilité du PAS....6
8 Mesures de sécurité et de protection....7
8.1 Organisation de la sécurité du SI titulaire....7
8.2 Organisation dans le cadre de la prestation....7
8.3 Achat....7
8.4 Formation et sensibilisation des intervenants....7
8.5 Gestion des incidents....8
8.6 Continuité de l'activité....8
8.7 Matrice de couverture des exigences de sécurité....9
9 Documentation de suivi....9
Nature du document....9
Date de remise....9
10 Annexes recommandées....9

1 Objet du PAS

Ce document constitue le Plan d'Assurance Sécurité (PAS) entre le titulaire et la DIR Centre-Est

Il décrit les dispositions que le titulaire du marché de maintenance des réseaux de transmission de la DIRCE s'engage à mettre en œuvre pour répondre aux exigences de sécurité de la DIRCE. Il définit en particulier l'organisation qui sera mise en place, les acteurs, les mesures et les procédures mis en œuvre par le titulaire pour assurer un niveau de sécurité en adéquation avec les enjeux de sécurité identifiés sur les réseaux de transmission de la DIRCE.

Le candidat précisera le circuit d'approbation du Plan d'Assurance Sécurité, ses modalités d'application et l'étendue de sa diffusion.

2 Documents de référence

Ce paragraphe liste les documents de référence pour le Plan d'Assurance Sécurité.

Les documents applicables sont :

- le CCTP
- le CCAP
- Le Plan d'Assurance sécurité

3 Rappel des exigences

Le candidat rappellera les exigences de sécurité annoncées par la DIRCE dans l'annexe 2 du CCTP.

4 Organisation et gouvernance

Le titulaire du marché précisera dans son offre la façon dont il prend en charge la Sécurité :

- au niveau de son organisation
- au niveau du marché

ainsi que les certifications et habilitations qu'il possède dans ce domaine.

Le candidat décrira précisément les mesures et dispositifs de sécurité mises en œuvre sur l'organisation des prestations.

Par dispositif, on entend les outils matériels, outils, méthodes, procédures mis en œuvre pour l'accomplissement de l'objectif.

Il précisera notamment :

- les dispositifs mis en place pour répondre aux exigences de protection des données à caractère personnel ;

- les dispositifs et outillages répondant aux exigences de sécurité décrits dans le CCTP et ses annexes ;
- les dispositifs techniques qu'il préconise pour échanger de façon sécurisée avec le CNRS (messagerie, transfert de fichier, livraison, etc.) ;
- les dispositifs techniques et organisationnels pour assurer la protection physique (environnementale, anti-intrusion, etc.) de ses locaux (un dossier de type site sûr annexé au plan d'assurance sécurité - PAS serait apprécié) ;
- les dispositifs techniques et organisationnels visant à sécuriser ses ressources informatiques (réseaux, postes de travail, smartphones, ressources partagées, messagerie, téléphonie, cloud, etc.) ;
- Les dispositifs techniques et organisationnels mis en œuvre visant à sécuriser et à protéger les ressources informatiques et accès logiques mis à disposition du titulaire par la DIRCE dans le cadre de la réalisation des prestations du présent marché ;
- les dispositifs organisationnels internes permettant de suivre la gestion, l'application et le contrôle des différents dispositifs mis en place.

Il est attendu que ces différents dispositifs soient au niveau de sécurité adéquat en regard à la sensibilité des informations traitées par les applications et projets dans le périmètre du marché.

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

Il décrira l'organisation mise en place pour assurer les relations avec le maître d'ouvrage concernant les aspects sécurité :

- comité de suivi de la sécurité : 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.

<u>Organisation de la maîtrise d'oeuvre :</u>

En tant que maître d'œuvre, le titulaire du marché 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 de sécurité. Il est rattaché directement au responsable de l'opération, au directeur de projet par exemple, désigné par le titulaire du marché.

Le responsable de la sécurité désigné par le titulaire du marché prend en charge l'organisation des comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes-rendus .

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

Organisation de la maîtrise d'ouvrage :

La DIRCE désignera un interlocuteur responsable de la sécurité du marché de maintenance des réseaux de transmission de la DIRCE. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour la DIRCE, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec le titulaire.

La sécurité globale du marché de maintenance des réseaux de transmission repose sur la participation active des différents intervenants : personnel interne qui avait un rôle dans le fonctionnement antérieur du système ou service faisant l'objet de l'opération d'externalisation [intégrateur, développeur, administrateur, exploitant, responsable technique, etc.], maîtrise d'ouvrage et maître d'oeuvre.

Le responsable de la sécurité désigné par la DIRCE a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'oeuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité lié à l'opération d'externalisation : politique de sécurité interne de la DIRCE, documentation technique du système [documents d'ingénierie, documents d'exploitation, etc.], spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'oeuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par le prestataire d'externalisation.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

Il identifie les risques de sécurité constatés sur l'infrastructure de la DIRCE.

5 Responsabilités liées au PAS

Le candidat, 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.

Il s'applique à l'ensemble des équipes de la maîtrise d'œuvre (et aux sous-traitants éventuels).

Sa rédaction relève du responsable sécurité désigné par le titulaire. Il doit être approuvé par la maîtrise d'ouvrage ; sa bonne exécution est de la responsabilité du titulaire en tant que maître d'oeuvre.

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

6 Procédure d’évolution du PAS

Le titulaire est responsable de la rédaction du PAS initial et de ses évolutions pour répondre aux exigences de sécurité du donneur d’ordres pendant toute la durée du contrat.

Voici une liste (non exhaustive) 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.
- Changement de représentant désigné pour la sécurité chez le titulaire ou à la DIRCE

En cas d’évolution du système, de son environnement, ou du périmètre du marché, le titulaire vérifie si le PAS doit être modifié. Si tel est le cas, il propose une modification à la DIRCE. Si cette modification est acceptée, le PAS est révisé et soumis à la DIRCE pour validation formelle.

Le responsable sécurité désigné par le titulaire 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 la maîtrise d’oeuvre. Cette révision sera réalisée par le responsable sécurité désigné par le titulaire. La version révisée du PAS sera transmise à la maîtrise d’ouvrage pour validation, et diffusée à l’ensemble des acteurs pour application.

7 Applicabilité du PAS

L’applicabilité du PAS s’articule autour des trois points suivants :

- quelles sont les procédures à suivre lors de non respect du PAS ?
- quelle est la procédure à suivre pour une demande de dérogation ?
- quelles sont les pénalités encourues ?

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.

Un acteur du projet identifiant un non respect du PAS dans ses procédures et mesures doit en référer immédiatement au titulaire, 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.

Un acteur du projet n’étant pas à même de remplir l’ensemble des clauses du PAS devra effectuer une demande de dérogation auprès du titulaire, qui négociera avec la DIRCE 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.

8 Mesures de sécurité et de protection

Le candidat décrira les mesures destinées à assurer la sécurité des matériels et des données liées au marché.

8.1 Organisation de la sécurité du SI titulaire

Le titulaire décrira l'organisation de la sécurité dans sa structure :

- Existence d'une PSSI
- Structure de l'organisation de la sécurité de Titulaire
- Nomination d'un Responsable de la Sécurité des Systèmes d'Information
- Formalisation des responsabilités SSI chez le Titulaire
- Séparation des rôles

8.2 Organisation dans le cadre de la prestation

Le titulaire décrira la manière dont il sera organisé pour gérer les missions liés à la sécurité dans la cadre du marché, notamment :

- Contact avec les autorités
- Contact avec les groupes de spécialistes
- Politique de sécurité de l'information pour les relations avec les tiers
- Intégration de la sécurité dans les contrats des tiers
- Cloisonnement avec les autres clients de Titulaire

8.3 Achat

Le candidat présentera dans ce paragraphe les mesures proposées pour sécuriser la phase d'achat de matériel (choix du fournisseur et du matériel proposé pour garantir le niveau de sécurité attendu)

8.4 Formation et sensibilisation des intervenants

Le candidat présentera dans ce paragraphe les mesures mises en place pour sensibiliser se agents et sous-traitants aux règles et bonnes pratiques en matière de sécurité. Il précisera notamment les mesures suivantes :

- Sélection des collaborateurs

- La charte sécurité (signée par l’ensemble des salariés)
- Clauses SSI dans les contrats de travail
- Responsabilités du management dans l'application de la SSI
- Engagement de sécurité des exploitants de Titulaire
- Sensibilisation et formation SSI des collaborateurs
- Sensibilisation et formation SSI des sous-traitants du titulaire
- Clauses de confidentialité - collaborateurs du Titulaire
- Clauses de confidentialité - sous-traitants du Titulaire

8.5 Gestion des incidents

Le candidat présentera les procédures de gestion des incidents de sécurité mise en place pour sa gestion interne des incidents :

- Rapports d’incidents
- Catégorisation des incidents
- Conservation des alarmes
- Collecte de preuves
- Chaîne de signalement des incidents et 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
- Définitions des alertes et incidents de sécurité
- Escalade et gestion de crise
- RACI et matrice des contacts en cas d’incident de sécurité

8.6 Continuité de l’activité

Le titulaire décrira la manière dont il gère la continuité de l’activité en cas d’incident de sécurité en précisant notamment l’existence des mesures suivantes et la manière dont elles sont implémentées :

- Résilience des dispositifs liés à la prestation
- Plan de Reprise d’Activité
- Plan de Continuité d’Activité
- Politique de sauvegarde
- Gestion des supports de sauvegarde

8.7 Matrice de couverture des exigences de sécurité

Le candidat présentera les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences du donneur d'ordres. Il pourra pour ce faire reprendre dans un tableau les exigences énoncées, et lister la ou les mesure(s) répondant à chaque exigence.

9 Documentation de suivi

Le candidat 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 (liste non exhaustive :

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	Lancement du marché
Plan de gestion des incidents	Début de phase d'exploitation
Comptes-rendus de réunion du comité de suivi	Une semaine après chaque réunion

10 Annexes recommandées

- Annexe 1 : Liste des personnes habilitées côté prestataire.
- Annexe 2 : Modèle de rapport d'incident sécurité.
- Annexe 3 : Modèle de matrice RACI sécurité (DIRCE/prestataire).