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 pare-feux de la DIR Centre-Est

Table des matières

Plan d'Assurance Sécurité....1
1 Objet du document....3
2 Documents de référence....3
3 Rappel des exigences....3
4 Organisation et gouvernance....3
4.1 Organisation de la sécurité du SI titulaire....3
4.2 Organisation dans le cadre de la prestation....4
4.3 Achat....4
4.4 Formation et sensibilisation des intervenants....4
5 La sécurité technique, physique et logique....5
6 La gestion des vulnérabilités....6
7 La gestion des incidents de sécurité....6
7.1 Procédure de gestion des incidents....6
7.2 Continuité de l'activité....7
8 La gestion de la réversibilité....7
9 Procédure d'évolution du PAS....7
10 Matrice de couverture des exigences de sécurité....8
11 Documentation de suivi....8
12 Annexes recommandées....8

1 Objet du document

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

Il décrit les dispositions que le titulaire du marché de maintenance des pare-feux 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 le chapitre 3 du CCTP.

4 Organisation et gouvernance

Le candidat précisera dans son offre la façon dont il prend en charge l'organisation et la gouvernance de la sécurité :

- au niveau de son organisation
- au niveau du marché

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

4.1 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

4.2 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

4.3 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)

4.4 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

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.

Organisation de la maîtrise d'oeuvre :

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 pare-feux 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 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.

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 La sécurité technique, physique et logique

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

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.

6 La gestion des vulnérabilités

Le candidat décrira le processus mis en place pour assurer le suivi des vulnérabilités concernant les matériels et logiciels couverts par le marché.

Il précisera notamment les processus mis en place pour:

- la veille et la détection des vulnérabilités (y compris les sources utilisées)
- l'analyse et qualification des vulnérabilités et des failles détectées
- la planification et l'arbitrage des mesures envisagées
- l'application des correctifs
- la vérification et le contrôle

7 La gestion des incidents de sécurité

Le Titulaire devra mettre en œuvre un processus documenté de gestion des incidents afin de détecter, qualifier, contenir et remédier à tout événement susceptible d'impacter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données et des systèmes de l'Acheteur ou le bon déroulement du marché.

A ce titre, le candidat décrira les processus mis en place pour la gestion des incidents de sécurité en interne et vis à vis de la DIRCE.

7.1 Procédure de 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

7.2 Continuité de l'activité

Le candidat 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 La gestion de la réversibilité

Le candidat indiquera les modalités techniques et les formats dans lesquels les données de la DIRCE seront restituées à la fin du marché puis détruites.

9 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.

10 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.

11 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 provisoire	**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**

12 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).