



Ministère de la Transition écologique et de la Cohésion des Territoires

Direction Générale des Infrastructures, des Transports et des Mobilités

Marché public relatif à la conception, la mise en service, l'exploitation, la commercialisation et le maintien en conditions opérationnelles et de sécurité du Service Numérique Multimodal Titre Unique (SNMTU) pour les phases d'expérimentation et de passage à l'échelle du projet Titre Unique

**ANNEXE 2 AU RÈGLEMENT DE LA CONSULTATION –
PLAN D'ASSURANCE SÉCURITÉ TYPE**

Numéro de consultation : DGITM-SDMINT-02-2024

Procédure de passation : Appel d'offres ouvert selon les dispositions des articles L.2124-1 et L.2124-2 et R.2124-2 et R.2161-2 à R.2161-5 du code de la commande publique.

Date limite de remise des offres : le 19 août 2024 à 12 h



Objet du document

Le plan-type proposé ci-après pourra être utilisé comme base de rédaction du Plan d'Assurance Sécurité qui sera fourni par les soumissionnaires en réponse à la consultation.

Article 1 - Objet du document

Ce document décrit les dispositions que <le prestataire d'externalisation> s'engage à mettre en oeuvre pour répondre aux exigences de sécurité de <le client>. 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 oeuvre.

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

Article 2 - Documents de référence

Ce paragraphe liste les documents de référence pour le 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 client ;
- le plan d'assurance qualité ;
- etc.

Article 3 - Description du système externalisé

Ce paragraphe présente succinctement le système faisant l'objet de l'opération d'externalisation. L'accent sera mis sur les points qui justifient la mise en oeuvre de mesures de sécurité.

Article 4 - Rappel des exigences

Le soumissionnaire rappellera les exigences de sécurité du client ou fera référence au document les spécifiant.

Article 5 - Organisation

Le soumissionnaire indiquera l'organisation qu'il propose pour gérer la sécurité dans le projet d'externalisation.

On y trouve au minimum :

- le maître d'ouvrage agissant en tant que client ;
- le prestataire d'externalisation.

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.



Organisation de la maîtrise d'oeuvre :

En tant que maître d'oeuvre, <le prestataire d'externalisation> 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 sécurité. Il est rattaché directement au responsable de l'opération, au directeur de projet par exemple, désigné par le <prestataire d'externalisation>.

Le responsable de la sécurité désigné par <le prestataire d'externalisation> prend en charge l'organisation des comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes-rendus [cf clause Comité de suivi].

Il pourra convier à ces réunions les intervenants impliqués dans les sujets inscrits à l'ordre du jour : sécurité applicative, sécurité des serveurs, sécurité des échanges...

Il conseille le client 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 :

<Le client> désignera un interlocuteur responsable de la sécurité du projet <projet d'externalisation>. Cet interlocuteur unique sera rattaché directement au directeur de projet. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour <le client>, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec le prestataire d'externalisation.

Des réunions de pilotage sécurité seront programmées tous les <période à évaluer>. Les participants à ces réunions pour <le client> seront le directeur du projet, le responsable de la sécurité, <liste à compléter> ainsi que le responsable technique ou fonctionnel lorsqu'ils sont impliqués dans les points à l'ordre du jour.

La sécurité globale de <l'opération d'externalisation> 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 <le client> 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 du <client>, 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.

Article 6 - Responsabilités liées au PAS

Le soumissionnaire, 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'oeuvre (et aux sous-traitants éventuels).

Sa rédaction relève du responsable sécurité désigné par <le prestataire d'externalisation>. Il doit être approuvé par la maîtrise d'ouvrage ; sa bonne exécution est de la responsabilité du <prestataire d'externalisation> 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).

Article 7 - 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.



En cas d'évolution du système, de son environnement, ou du périmètre de l'opération d'externalisation, le titulaire vérifie si le PAS doit être modifié. Si tel est le cas, il propose une modification au client. Si cette modification est acceptée, le PAS est révisé et soumis au client pour validation formelle.

Le responsable sécurité désigné par <le prestataire d'externalisation> 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 prestataire d'externalisation>. La version révisée du PAS sera transmise à la maîtrise d'ouvrage pour validation, et diffusée à l'ensemble des acteurs pour application.

Article 8 - 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 <prestataire d'externalisation>, 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 prestataire d'externalisation> 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 du <prestataire d'externalisation>, qui négociera avec <le client> 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.

Article 9 - Mesures de sécurité

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, phase d'exploitation, phase de réversibilité ou fin de contrat.

9.1 Transfert

Le soumissionnaire présentera dans ce paragraphe les mesures proposées pour sécuriser la phase de transfert du système (transfert de matériels ou de logiciels dans un projet d'externalisation) [cf clause de transfert].

Il décrira les procédures de contrôle de la sécurité du transfert mises en oeuvre et identifiera ses obligations de reporting au comité de suivi sécurité [cf clause de contrôle des prestations et des résultats].

Les exigences de sécurité formulées par le client indiquent le niveau de confidentialité maximum des informations manipulées notamment lors du transfert. Une liste de personnes susceptibles de participer au transfert pourra être rédigée et communiquée au client. Le client devra indiquer s'il juge nécessaire que le personnel soit soumis à une clause de confidentialité ou procéder à une habilitation [cf clause de confidentialité].

9.2 Exploitation

Le soumissionnaire présentera dans ce paragraphe les mesures mises en place pour assurer la protection du système externalisé en réponse aux exigences identifiées par le client.



9.3. Réversibilité

Le soumissionnaire s'engagera à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le client, ou par un autre prestataire de service [cf clause de réversibilité].

Article 10 - Matrice de couverture des exigences de sécurité

Le soumissionnaire 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.

Article 11 - Documentation 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. 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