

Direction du Numérique et des Systèmes d’Information

**Pouvoir Adjudicateur :**

Agence de services et de paiement (ASP)

2, rue du Maupas

87 040 LIMOGES cedex 1

Annexe n° 3 du CCAP

Plan d’Assurance Sécurité (PAS), plan type

**MP 25-01 : Prestations de dématérialisation de documents et de RAD-LAD (Reconnaissance Automatique de Documents - Lecture Automatique de Documents)**

SOMMAIRE

[Article 1. Approbation du PAS 3](#_Toc133509341)

[Article 2. Documents de référence 3](#_Toc133509342)

[Article 3. Description du dispositif 3](#_Toc133509343)

[Article 4. Rappel des exigences 3](#_Toc133509344)

[Article 5. Organisation 3](#_Toc133509345)

[Article 6. Responsabilités liées au PAS 3](#_Toc133509346)

[Article 7. Procédure d’évolution du PAS 4](#_Toc133509347)

[Article 8. Applicabilité du PAS 4](#_Toc133509348)

[Article 9. Mesures de sécurité 4](#_Toc133509349)

[Article 10. Matrice de couverture des exigences de sécurité 5](#_Toc133509350)

[Article 11. Documentation et suivi 5](#_Toc133509351)

# Approbation du PAS

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

# Documents de référence

Ce paragraphe listera les documents de référence, applicables pour le Plan d’Assurance Sécurité.

* Le contrat ;
* Le cahier des charges ;
* Etc.

# Description du dispositif

Ce paragraphe présente succinctement le dispositif, objet de la prestation. L’accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité.

# Rappel des exigences

Le titulaire rappellera les exigences de sécurité de l’ASP ou fera référence au document les spécifiant.

# Organisation

Le titulaire indiquera l’organisation qu'il propose pour gérer la sécurité dans le projet, avec au minimum :

* Le maître d’ouvrage agissant en tant que client ;
* Le titulaire du marché/contrat.

Si des cotraitants, 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 titulaire : responsable sécurité, rôle et moyens ; responsables techniques, implication des cotraitants 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.

# Responsabilités liées au PAS

Le titulaire, 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.

# 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 de l’ASP, pendant toute la durée du marché/contrat.

La liste (non exhaustive) des situations susceptibles d’entraîner une modification du PAS :

* Evolution du système d’information (configuration logicielle ou matérielle) ;
* Evolution de l’environnement du système d’information (locaux, personnels, procédures, etc.) ;
* Evolution 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 à l’ASP dans un délai de x jours ouvrés, avant la mise en application. Si cette modification est acceptée, le PAS est révisé et soumis à l’ASP pour validation formelle.

# 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?

# Mesures de sécurité

Le titulaire décrira les mesures destinées à assurer la sécurité du système cible de l’opération pendant les différentes phases contractuelles :

* Transfert ;
* Exploitation ;
* Réversibilité ;
* Fin de marché.

**Sécurité physique**

* Isolement des locaux dédiés à la prestation de l’ASP ;
* protections contre l'intrusion ;
* protections contre l'incendie.

**Contrôle d'accès physique**

* Description du dispositif ;
* Procédure d'attribution/suppression/contrôle des droits d'accès aux locaux ;
* Traçage ;
* Liste initiale des accès attribués.

**Sécurité du poste de travail**

* Méthode d'accès aux postes (règles et méthode d'identification/authentification) ;
* Règles spécifiques de mot de passe (longueur, complexité, blocage ...) ;
* Système de mise à jour (OS et middleware) ;
* Protection Antivirus (produit, méthode de mise à jour et de surveillance) ;
* Règles de renforcement de sécurité du poste de travail (firewall local, gestion des ports/services, prise de main à distance ...) ;
* Mise en veille forcée ;
* Non enregistrement des mots de passe dans les navigateurs.

**Sécurité réseau**

* Synoptique du réseau LAN et WAN, incluant accès ASP et services internes ;
* Matrice des flux de l'accès aux ressources non protégées (accès Web, Messagerie, Mise à jour Windows, Mises à jour antivirus, services d'impression ...) ;
* Configuration des équipements de sécurité (règles entre réseau entreprise et réseau dédié ASP).

**Arrivée - départ d'un agent**

* Organisation générale ;
* Signature de la charte utilisateur ;
* Attribution / modification / suppression des droits d'accès physiques et logiques ;
* Communication des éléments à l’ASP.

**Télétravail**

Rappel : le télétravailleur n'accède jamais directement aux ressources ASP, mais via un rebond par le site du titulaire.

* Décrire organisation générale ;
* Modalité technique (entre site tiers et site du titulaire) ;
* Synoptique du réseau ;
* Postes, logiciels et algorithmes utilisés ;
* Supervision.

**Continuité d’activité**

* Description des moyens techniques mis en œuvres (locaux de repli, serveurs, postes de travail, réseaux ...) ;
* L'organisation mise en place (procédures de déclenchement, procédures de reprise).

# Matrice de couverture des exigences de sécurité

Le titulaire présentera les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences de l’ASP.

Il pourra pour ce faire reprendre dans un tableau les exigences énoncées, et lister la ou les mesure(s) répondant à chaque exigence.

# Documentation et suivi

Le titulaire 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 : Plan d’Assurance Sécurité (version 1 et définitive), Dossier de sécurité, Plan de secours, plan de gestion des incidents, comptes rendus de réunion du comité de suivi.