**Secrétariat général du Gouvernement et**

**Direction de l’information légale et administrative**

**CADRE DE REPONSE PLAN ASSURANCE SECURITE**

**Template 1.0.3**

**Société :**

**Projet :**

**Cadre de la réponse : préciser le marché, le périmètre le cas échéant**

Table des matières

[Suivi des versions 3](#_Toc109914538)

[Préambule 4](#_Toc109914539)

[1 Description de la prestation 5](#_Toc109914540)

[1.1 Glossaire et définitions 5](#_Toc109914541)

[1.2 Documents de référence et associés 5](#_Toc109914542)

[1.3 Périmètre du « plan assurance sécurité » 5](#_Toc109914543)

[2 Exigences de sécurité 5](#_Toc109914544)

[2.1 Sécurité des ressources humaines 5](#_Toc109914545)

[2.2 Gestion des actifs 5](#_Toc109914546)

[2.3 Gestion des accès logiques 5](#_Toc109914547)

[2.4 Gestion des authentifiants 6](#_Toc109914548)

[2.5 Sécurité physique 6](#_Toc109914549)

[2.6 Sécurité de l’exploitation des SI 6](#_Toc109914550)

[2.7 Sécurité des communications 6](#_Toc109914551)

[2.8 Sécurité des développements 6](#_Toc109914552)

[2.9 Maintenance des SI 7](#_Toc109914553)

[2.10 Relation avec les tiers 7](#_Toc109914554)

[2.11 Gestion des incidents et des alertes 7](#_Toc109914555)

[2.12 Gestion de la continuité d’activité 7](#_Toc109914556)

[2.13 Mise à jour des systèmes et logiciels 7](#_Toc109914557)

[2.14 Gestion de la documentation 8](#_Toc109914558)

[2.15 Contrôle et évaluation 8](#_Toc109914559)

[3 Organisation de la sécurité 8](#_Toc109914560)

[4 Responsabilités liées au PAS 8](#_Toc109914561)

[5 Procédures d’évolution du PAS 8](#_Toc109914562)

[6 Mesures de sécurité 8](#_Toc109914563)

[7 Couverture des exigences de sécurité 8](#_Toc109914564)

[8 Documentation de suivi 9](#_Toc109914565)

# Préambule

Le présent document est le cadre de réponse pour le plan d’assurance sécurité que les soumissionnaires doivent impérativement respecter pour constituer leur réponse.

Ce document ne concerne que la sécurité des systèmes d’information associée au marché 26\_BAM\_695, Prestations de restauration au bénéfice de la Direction de l’information légale et administrative (DILA), site Desaix. Dans le cadre d’une sous-traitance, ce document sera rempli par le fournisseur de la solution informatique.

Le respect des indications du présent cadre technique et plus généralement des exigences est pris en compte dans le critère « Cohérence et conformité de la réponse du soumissionnaire ».

Il définit les chapitres qui devront être présents dans leur mémoire technique. Les chapitres doivent être nommés de manière identique et présentés dans le même ordre que ceux présentés dans le tableau ci-dessous. Tout chapitre ne respectant ces règles et tout chapitre supplémentaire ajouté à l’initiative d’un soumissionnaire ne sera pas pris en compte dans l’évaluation de l’offre.

Les soumissionnaires sont libres de joindre des documents annexes permettant de mieux apprécier leur offre technique. Le pouvoir adjudicateur n’a toutefois aucune obligation d’en tenir compte pour l’évaluation des offres.

Les soumissionnaires veillent à faire des réponses concises et précises.

Pour chaque section, le soumissionnaire démontre sa capacité à répondre aux exigences du cahier des charges et à être une force de proposition réactive et proactive, sans se limiter aux éléments énoncés dans le CCTP. Il fournit quand cela est possible des exemples concrets, des schémas clairs en plus des explications et des engagements pris. Il s’attache à démontrer la qualité de son organisation pour décrire l’ensemble des actions spécifiques à mettre en œuvre lors de l’exécution du marché pour garantir le respect des exigences de sécurité. A ce titre, le répondant explicite les méthodologies utilisées et décrire les moyens techniques, organisationnel et humain mis en œuvre pour maintenir un niveau de sécurité optimum.

Le modèle proposé reprend les principales thématiques permettant de s’assurer du bon niveau de prise en compte de la sécurité des systèmes d’information. Les rubriques ci-dessous sont, dans le cas du présent marché, données à titre indicatif. Si certaines informations sont jugées nécessaires par l’acheteur, il se réserve le droit de poser les questions afférentes au soumissionnaire.

# Description de la prestation

## Glossaire et définitions

Aide pour compléter le dossier (à effacer)

Ajouter ici les informations nécessaires à la bonne compréhension des termes mentionnés dans le document.

## Documents de référence et associés

Aide pour compléter le dossier (à effacer)

Lister ici tous les documents auquel le PAS fait référence. Pour les documents qui ne sont pas fournis par la DILA, expliquer en quelques mots le sujet du document mentionné.

## Périmètre du « plan assurance sécurité »

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments de la prestation couverts par le plan d’assurance qualité.

# Exigences de sécurité

## Sécurité des ressources humaines

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants afin de s’assurer que les personnes en charge du système d’information sont à même d’assurer le niveau de prestation attendu :

* Recrutement
* Gestion des arrivées départ
* Sensibilisation et formation à la SSI

## Gestion des actifs

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Cartographie des actifs
* Classification des actifs
* Protection des informations

## Gestion des accès logiques

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Droits d’accès aux ressources
* Contrôle d’accès logique aux SI
* Gestion des habilitations
* Gestion des sessions inactives
* Traçabilité des accès

## Gestion des authentifiants

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Gestion des mots de passe
* Gestion des certificats

## Sécurité physique

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Contrôle d’accès physique aux locaux
* Traçabilité des accès physiques aux locaux
* Protection des zones de sécurité physique

## Sécurité de l’exploitation des SI

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Durcissement des ressources informatiques
* Sauvegardes et restauration
* Documentation des ressources informatiques
* Gestion des correctifs de sécurité
* Lutte contre les codes malveillants
* Administration des SI

## Sécurité des communications

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Politique de sécurité des communications
* Sécurisation des transmissions de données
* Accès à distance aux SI
* Accès au réseau interne depuis des équipements non maîtrisés

## Sécurité des développements

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Règles de développement
* Cloisonnement des environnements
* Données d’essai
* Gestion des évolutions
* Suivi et prise en compte des alertes sécurités (notamment sur les bibliothèques utilisées)
* Réalisation d’audit interne ou externe sur les applications

## Maintenance des SI

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Maintien du niveau de sécurité des SI
* Sécurité de la maintenance des SI
* Mise au rebut

## Relation avec les tiers

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Gestion de la sécurité avec les sous-traitants

## Gestion des incidents et des alertes

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Veille et gestion des vulnérabilités techniques
* Détection et dispositif de gestion des incidents
* Journalisation des incidents et des alertes
* Gestion de crise

## Gestion de la continuité d’activité

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Définition, mise en œuvre et maintien du plan de continuité d’activité
* Protection des données de sauvegarde

## Mise à jour des systèmes et logiciels

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Sécurité des postes de travail
* Utilisation de terminaux personnels
* Privilèges des utilisateurs sur les postes de travail
* Stockage des informations
* Protection des données critiques
* Configuration du navigateur internet

## Gestion de la documentation

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Référentiel documentaire
* Gestion de la documentation

## Contrôle et évaluation

Aide pour compléter le dossier (à effacer)

Décrire ici en quelques mots les éléments mis en œuvre sur les sujets suivants :

* Contrôles récurrents de conformité à la PSSI
* Audits ponctuels de conformité à la PSSI
* Reporting SSI

# Organisation de la sécurité

Aide pour compléter le dossier (à effacer)

Décrire comment est organisée la sécurité au sein des équipes projet (processus, couverture…)

# Responsabilités liées au PAS

Aide pour compléter le dossier (à effacer)

*Lister les différentes personnes / rôles ayant une responsabilité dans la mise en œuvre du PAS ainsi que leur périmètre d’intervention.*

# Procédures d’évolution du PAS

Aide pour compléter le dossier (à effacer)

Décrire les procédures envisagées pour faire évoluer le PAS, soit à la demande du titulaire, soit à la demande de l’acheteur

# Mesures de sécurité

Aide pour compléter le dossier (à effacer)

Décrire ici les mesures de sécurité mises en place dans le marché. Ce point englobe aussi la manière dont il est envisagé par le titulaire de réaliser un développement sécurisé by design.

# Couverture des exigences de sécurité

Aide pour compléter le dossier (à effacer)

Mettre ici un tableau regroupant les mesures de sécurité demandées et leur niveau de couverture (justifier les réponses) :

* - : non couvert ;
* \* : partiellement couvert
* \*\* : complètement couvert

Le tableau pourra être construit sur la base de la PSSIE, le guide d’architecture technique et les bonnes pratiques référencées sur le site de l’ANSSI.

# Documentation de suivi

Aide pour compléter le dossier (à effacer)

Lister, joindre et décrire en quelque ligne les différents documents sur lesquels la répondant s’appuie pour suivre le plan d’assurance sécurité proposé.

Cela peut couvrir selon l’organisation mise en place des documents contractuels avec un hébergeur, les documents de références sur lesquels le répondant s’appuie pour mener à bien son plan d’assurance qualité.