

# EXIGENCES SSI

Marché de maquettage éditorial

Version 1.1

Diffusion restreinte

Les exigences SSI du présent document visent à garantir :

|                                     |                         |                           |
|-------------------------------------|-------------------------|---------------------------|
| ✓ Confidentialité avant publication | ✓ Maîtrise des accès    | ✓ Sécurisation des outils |
| ✓ Traçabilité des actions           | ✓ Gestion des incidents | ✓ Destruction maîtrisée   |

## 1. Contexte de la prestation

### Objet du marché

Le Service statistique ministériel de la sécurité intérieure (SSMSI) confie au titulaire des prestations de maquettage éditorial, création graphique, secrétariat de rédaction et coordination de projet pour ses publications et supports de communication.

### Sensibilité particulière

Le titulaire est amené à recevoir, traiter, stocker et échanger des textes, tableaux, chiffres, figures, fichiers sources et versions intermédiaires AVANT publication officielle. Ces éléments sont soumis à des exigences strictes de protection.

## 2. Vue d'ensemble des domaines SSI

Le dispositif SSI s'articule autour de 9 domaines complémentaires, chacun portant des exigences spécifiques et des livrables attendus du titulaire.

| # | Domaine                                           | Objectif principal                                                                                       |
|---|---------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| A | Confidentialité & embargo                         | Protection stricte des contenus avant publication officielle                                             |
| B | Plan d'Assurance Sécurité (PAS)                   | Cadre documenté des mesures de sécurité organisationnelles et techniques                                 |
| C | Hébergement, stockage & outils                    | Maîtrise des environnements numériques et de la localisation des données                                 |
| D | Gestion des versions et nomenclature documentaire | Maîtrise des versions, identification du BAT (Bon À Tirer) validé et prévention des erreurs de diffusion |
| E | Comptes, habilitations & traçabilité              | Contrôle des accès individualisés et traçabilité des actions                                             |

|          |                                                    |                                                                        |
|----------|----------------------------------------------------|------------------------------------------------------------------------|
| <b>F</b> | <b>Postes de travail &amp; mobilité</b>            | Sécurisation des équipements fixes et mobiles utilisés pour le marché  |
| <b>G</b> | <b>Sauvegarde et continuité</b>                    | Garantie de la disponibilité et de la reprise des données              |
| <b>H</b> | <b>Incidents &amp; audit</b>                       | Détection, signalement et remédiation des incidents de sécurité        |
| <b>I</b> | <b>Gestion des personnels &amp; sous-traitants</b> | Responsabilité étendue à l'ensemble des intervenants et sous-traitants |

### 3. Exigences par domaine

#### **A Confidentialité, embargo et protection de l'information**

Le titulaire est tenu à une obligation stricte de confidentialité sur l'ensemble des documents, fichiers, supports et échanges. Il applique le principe du besoin d'en connaître et s'interdit toute réutilisation ou diffusion hors marché.

#### Livrables attendus

| Document à fournir                                                  | Détails                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Engagement formel de confidentialité et de respect de l'embargo     | Document signé par le représentant du titulaire, couvrant la confidentialité, le non-usage hors marché, la non-divulgateion, la limitation des copies et le respect de l'embargo, avec extension explicite à tous les intervenants du marché. |
| Inventaire des documents et fichiers SSMSI détenus par le titulaire | Inventaire à jour des documents, fichiers, versions et supports du SSMSI détenus par le titulaire, précisant leur nature, leur version, leur localisation et, le cas échéant, leur statut.                                                    |
| Procès-verbal de restitution des éléments                           | Procès-verbal listant précisément les éléments restitués au SSMSI.                                                                                                                                                                            |
| Procès-verbal de destruction                                        | Procès-verbal précisant les éléments détruits, la date, les moyens de destruction utilisés et certifiant qu'aucune copie résiduelle n'a été conservée.                                                                                        |

#### Remise des documents

L'engagement de confidentialité et la liste des intervenants autorisés sont remis **avant tout accès aux documents du marché**. La liste est mise à jour en cas d'évolution. Les procès-verbaux de restitution et de destruction sont remis **en fin de prestation**, à la première demande du SSMSI ou à l'issue des opérations concernées. L'inventaire des documents est remis **au démarrage si des documents sont déjà détenus**, puis tenu à jour pendant toute la durée du marché.

## B Plan d'Assurance Sécurité (PAS)

### Document de référence

Le PAS constitue le document central du dispositif de sécurité du titulaire. Il doit être daté, versionné, cohérent avec le périmètre réel et tenu à jour pendant toute la durée du marché. Toute évolution significative doit donner lieu à une mise à jour préalablement validée par le SSMSI.

### Livrables attendus

| Document à fournir        | Détails                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plan d'Assurance Sécurité | PAS daté, versionné et transmis officiellement par le titulaire.                                                                                                                        |
| Mises à jour du PAS       | Toute mise à jour du PAS résultant d'un changement significatif affectant les outils, les intervenants, les accès, le stockage, la localisation des données ou les mesures de sécurité. |

### Remise des documents

Le PAS est remis au **démarrage des prestations**. Toute mise à jour du PAS est transmise avant sa mise en application, dès qu'un changement significatif affecte le dispositif de sécurité du marché.

## C Hébergement, stockage, outils et localisation

Le titulaire déclare l'ensemble des modalités d'hébergement, de stockage, de partage, de sauvegarde et de traitement des données. Il veille à la séparation effective des données du SSMSI de ses propres données et de celles de ses autres clients.

Les données du marché, y compris les données en exploitation, les sauvegardes, les copies, les archives et les répliques éventuelles, **doivent être hébergées au sein de l'Union européenne**. Lorsqu'un service cloud est utilisé dans le cadre du marché, le service d'hébergement ou de traitement concerné doit bénéficier d'une qualification SecNumCloud, ou d'un niveau de garanties équivalent, dûment justifié par le titulaire et validé par le SSMSI.

Tout recours à un hébergement situé hors de ce périmètre, ou à un prestataire impliquant un traitement ou un stockage des données en dehors de ce périmètre, est subordonné à une étude préalable et à une validation du SSMSI.

Tout recours à un service tiers non validé par le SSMSI, notamment à un **outil d'intelligence artificielle générative, est interdit** pour le traitement, l'analyse, la reformulation, l'illustration ou le stockage de contenus du marché non publiés.

**Livrables attendus**

| Document à fournir                                                         | Détails                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Déclaration des outils utilisés                                            | Fiche de déclaration des outils utilisés dans le cadre du marché, précisant pour chaque outil : nom, éditeur, finalité, type de données traitées, environnement d'usage, administration, stockage, sauvegarde et mesures de sécurité associées.                                                                                                                                                                                                                                                                                                       |
| Fiche d'hébergement et de localisation des données                         | Fiche précisant le ou les hébergeurs concernés, la nature du service utilisé, la localisation des données, des sauvegardes, des copies, archives ou répliques éventuelles et, le cas échéant, les sous-traitants techniques impliqués. Lorsque le marché repose sur un service cloud, cette fiche indique si le service utilisé bénéficie d'une qualification SecNumCloud ou d'un niveau de garanties équivalent. Toute situation impliquant un traitement ou un stockage hors de l'Union européenne doit y être explicitement signalée et justifiée. |
| Déclaration des services tiers et engagement de non-usage d'IA non validée | Document précisant les services tiers utilisés dans le cadre du marché et engagement du titulaire interdisant l'usage d'outils d'IA générative ou de services non validés pour traiter des contenus SSMSI non publiés.                                                                                                                                                                                                                                                                                                                                |
| Note de séparation des données                                             | Note précisant comment les données du SSMSI sont isolées de celles du titulaire, de ses autres clients et de ses autres espaces ou projets internes.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Note sur les modalités d'échange sécurisées                                | Note précisant les canaux autorisés, les règles de partage, les restrictions d'accès, les protections mises en œuvre pour garantir la confidentialité et l'intégrité des échanges.                                                                                                                                                                                                                                                                                                                                                                    |

**Remise des documents**

Les éléments du présent bloc, lorsqu'ils concourent à l'appréciation de la conformité de l'offre, **sont attendus dès la réponse du titulaire**. Ils sont ensuite confirmés, complétés ou actualisés avant l'utilisation des outils ou services concernés. Ils sont mis à jour sans délai en cas d'évolution des outils, de l'hébergement, de la localisation des données, des modalités de stockage ou des canaux d'échange.

**D****Gestion des versions et nomenclature documentaire**

Le titulaire met en œuvre une organisation documentaire permettant d'identifier sans ambiguïté la version de référence de chaque livrable du marché, de tracer les versions intermédiaires et de sécuriser les allers-retours de correction jusqu'au BAT.

Il applique une nomenclature claire des fichiers, centralise les retours dans un canal validé par le SSMSI et veille à prévenir tout risque d'erreur, de confusion ou d'utilisation d'une version obsolète.

**Livrables attendus**

| Document à fournir           | Détails                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Note de gestion des versions | Note décrivant le cycle de versionnement appliqué au marché, depuis la première version de travail jusqu'au BAT, en précisant les statuts utilisés, les règles de validation et le traitement des versions intermédiaires. |

|                                           |                                                                                                                                                                                         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nomenclature documentaire                 | Règles de nommage des fichiers, précisant les conventions retenues pour identifier le document, la version, la date, le statut et, le cas échéant, le périmètre ou le support concerné. |
| Identification de la version de référence | Document ou règle précisant comment la version de référence est identifiée à chaque étape, notamment pour les versions transmises au SSMSI et pour le BAT validé.                       |

**Remise des documents**

Les éléments du présent bloc, lorsqu'ils concourent à l'appréciation de la conformité de l'offre, **sont attendus dès la réponse du titulaire**. Ils sont ensuite confirmés, complétés ou actualisés au démarrage des prestations. Ils sont mis à jour en cas d'évolution du processus documentaire, des outils utilisés ou des modalités de validation, et appliqués pendant toute la durée du marché. La version de référence et le BAT validé doivent pouvoir être identifiés à tout moment à la demande du SSMSI.

## E Comptes, habilitations et traçabilité

**Principe du moindre privilège**

Les accès sont nominatifs et individualisés. Les droits sont attribués selon le principe du moindre privilège. Les comptes obsolètes sont supprimés sans délai. Des traces horodatées et imputables sont conservées pour toutes les actions.

**Livrables attendus**

| Document à fournir                                        | Détails                                                                                                                                                                                                                                |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Matrice des comptes et habilitations                      | Liste des personnes pouvant accéder aux documents du SSMSI, pour chaque intervenant, son identité, son rôle, les outils ou espaces accessibles, le niveau d'accès et, le cas échéant, les dates d'ouverture et de fermeture des accès. |
| Procédure de gestion des arrivées, départs et changements | Procédure décrivant la création des comptes, l'attribution des droits, la modification des habilitations, la désactivation ou suppression des comptes et le traitement des départs et fins d'intervention.                             |
| Note sur la conservation des traces (journaux)            | Attestation ou note précisant la durée de conservation des journaux et les modalités de protection des traces.                                                                                                                         |

**Remise des documents**

Les éléments du présent bloc, lorsqu'ils concourent à l'appréciation de la conformité de l'offre, **sont attendus dès la réponse du titulaire**. Ils sont ensuite confirmés, complétés ou actualisés au démarrage des prestations. Ils sont mis à jour en cas d'évolution des accès, des intervenants ou des règles de gestion, et tenus à disposition du SSMSI pendant toute la durée du marché.

**F****Postes de travail et mobilité**

Le titulaire met en œuvre un niveau de sécurité adapté sur tous les postes (fixes et mobiles) utilisés pour le marché. Le chiffrement est obligatoire. Le verrouillage automatique de session est requis.

**Livrables attendus**

| Document à fournir                                   | Détails                                                                                                                                                                                                                                      |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attestation de conformité des postes utilisés        | Attestation couvrant l'identification des postes fixes et mobiles utilisés pour le marché, ou à minima des catégories de postes autorisées, et confirmant qu'ils sont maintenus dans un état de sécurité satisfaisant, cohérent avec le PAS. |
| Preuve de chiffrement des postes                     | Confirmation que tous les postes stockant, traitant ou échangeant des documents SSMSI sont chiffrés, en particulier les postes nomades. Cette preuve peut être intégrée à l'attestation de conformité si elle y figure explicitement.        |
| Note de protection des postes nomades et de mobilité | Note précisant les mesures applicables aux équipements mobiles : prévention perte/vol, sécurisation physique, confidentialité de l'affichage, limitation du stockage local et conduite à tenir en cas d'incident sur un poste nomade.        |

**Remise des documents**

Ces éléments sont remis au **démarrage des prestations**. Ils sont mis à jour en cas d'évolution significative du parc, des équipements utilisés ou des modalités de travail en mobilité.

**G****Sauvegarde et continuité**

Le titulaire garantit la continuité des prestations et la préservation des données pendant toute la durée du marché. Il assure des sauvegardes adaptées et, le cas échéant, réalise des tests de restauration.

**Livrables attendus**

| Document à fournir                                   | Détails                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Note de continuité d'activité                        | Note de continuité d'activité ou extrait du PCA (Plan de Continuité d'Activité) applicable au marché, précisant les données couvertes, les outils concernés, les scénarios d'indisponibilité pris en compte, les modalités de reprise et les relais prévus en cas d'indisponibilité d'un poste, d'un outil ou d'un intervenant. |
| Note de sauvegarde                                   | Note précisant ce qui est sauvegardé, la fréquence, le support ou service utilisé, la localisation des sauvegardes, les protections appliquées et la durée de conservation.                                                                                                                                                     |
| Compte rendu de test de restauration (si applicable) | Élément justifiant la réalisation des tests de restauration, précisant la date, le périmètre testé, le résultat et, le cas échéant, les anomalies constatées.                                                                                                                                                                   |

**Remise des documents**

Ces éléments sont remis au **démarrage des prestations**. Ils sont mis à jour en cas d'évolution des outils, des modalités de sauvegarde, des conditions de continuité ou du périmètre des données couvertes.

**H****Incidents et audit****Canal dédié d'alerte sécurité**

Le titulaire met en place un canal dédié pour assurer une information rapide, fiable et traçable du SSMSI sur tout événement susceptible d'affecter les données, documents ou outils du marché. Des fiches réflexes couvrent les scénarios plausibles.

**Scénarios couverts par les fiches réflexes**

|                               |                                           |                           |
|-------------------------------|-------------------------------------------|---------------------------|
| ✓ Fuite ou suspicion de fuite | ✓ Erreur de diffusion                     | ✓ Perte ou vol d'un poste |
| ✓ Compromission d'un compte   | ✓ Indisponibilité d'un outil collaboratif | ✓ Code malveillant        |

**Livrables attendus**

| Document à fournir                                   | Détails                                                                                                                                                                                                                                                             |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fiche de contact sécurité                            | Fiche précisant le canal utilisé pour les alertes, les coordonnées des points de contact, les modalités de joignabilité et les règles d'escalade.                                                                                                                   |
| Procédure de signalement et de gestion des incidents | Procédure écrite couvrant la détection, l'alerte, la qualification, les mesures conservatoires, l'analyse, la clôture et les responsabilités associées.                                                                                                             |
| Attestation de prise en compte du droit d'audit      | Document par lequel le titulaire reconnaît le droit du SSMSI à réaliser ou faire réaliser des contrôles et audits sur le périmètre du marché.                                                                                                                       |
| Fiches réflexes incident                             | Fiches réflexes applicables aux principaux scénarios plausibles du marché, notamment fuite ou suspicion de fuite, erreur de diffusion, perte ou vol d'un poste, compromission d'un compte, indisponibilité d'un outil collaboratif ou présence de code malveillant. |

**Remise des documents**

Ces éléments sont remis au **démarrage des prestations**. Ils sont mis à jour en cas d'évolution du dispositif, des contacts ou des scénarios d'incident, et utilisés sans délai en cas d'événement de sécurité.

## I Gestion des personnels et des sous-traitants

Le titulaire demeure pleinement responsable de l'ensemble des personnes mobilisées (salariés, freelances, renforts, sous-traitants). Il désigne un responsable sécurité SI (Systèmes d'Information) dédié, interlocuteur privilégié du SSMSI.

### Livrables attendus

| Document à fournir                                        | Détails                                                                                                                                                                        |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preuve d'extension des obligations SSI aux sous-traitants | Engagements de confidentialité et de sécurité signés par les sous-traitants ou intervenants externes, ou document démontrant que les mêmes obligations SSI leur sont imposées. |
| Désignation du responsable sécurité                       | Document de désignation du responsable sécurité SI, avec ses coordonnées et une description synthétique de son rôle.                                                           |
| Preuve de sensibilisation SSI des intervenants            | Attestation de sensibilisation SSI ou relevé indiquant les thèmes couverts, les personnes sensibilisées, la date et le support utilisé.                                        |

### Remise des documents

Ces éléments sont remis **avant toute intervention sur le marché**. Ils sont mis à jour en cas de changement d'intervenant, de sous-traitant ou de responsable sécurité, et la preuve de sensibilisation est renouvelée si nécessaire en fonction des évolutions de l'équipe ou du dispositif.

## 4. Modalités générales de remise

### **Principe général**

Les éléments demandés sont transmis selon le calendrier indiqué pour chaque rubrique, et au plus tard 5 jours ouvrés avant le démarrage effectif des prestations pour les éléments dus au démarrage, sauf indication contraire. Pour les blocs C, D et E, les éléments concourant à l'appréciation de la conformité de l'offre sont attendus dès la réponse du titulaire, puis confirmés, complétés ou actualisés au démarrage des prestations. Les documents restent tenus à jour pendant toute la durée du marché. Le titulaire informe sans délai le SSMSI de toute évolution affectant les intervenants, les outils, les modalités de stockage, les accès ou les dispositifs de sécurité.

### **En cas d'impossibilité de fournir un élément**

Le titulaire informe sans délai le SSMSI et produit une justification écrite précisant :

- L'élément concerné et le motif de l'impossibilité
- Le caractère temporaire ou définitif de l'impossibilité
- Les mesures compensatoires éventuellement mises en œuvre
- Le délai prévisionnel de transmission si applicable

### **Réserve du SSMSI**

Le SSMSI se réserve la possibilité d'apprécier toute justification, de demander tout élément complémentaire et d'exiger, si nécessaire, une mesure compensatoire ou une preuve alternative.

