

Annexe 1 au CCTP – Marché 2024-0319

Exigences MANDATORY en lien avec la Sécurité des Systèmes d'Information

I. Documentation applicable

Les titulaires des différents lots s'engagent, sur leurs périmètres respectifs, à suivre et à mettre en application les référentiels d'exigences et guides listés ci-après :

- Politique Générale de la Sécurité du Numérique du Ministère de l'Intérieur (PGSN MI v1.0) ainsi que ses différentes annexes
- Politique Générale de la Sécurité du Numérique de France Titres (PGSN France Titres v1.0) ainsi que ses différentes annexes
- Référentiel général de sécurité (RGS – version 2.0 | [lien](#))
- Guide externalisation de l'ANSSI ([lien](#))

L'ensemble de ces documents sera fourni au futur titulaire du marché, et les informations qu'ils contiennent sont réputées connues du titulaire comme de ses agents qu'il aura déclarés à l'ANTS préalablement à tout commencement d'exécution du lot concerné. Le titulaire s'engage à respecter, et faire respecter par ses agents, l'ensemble des obligations détaillées.

En cas de défaillance constatée dans la mise en œuvre de mesures de sécurité en adéquation avec le niveau de sensibilité des données traitées, il pourra être fait obligation au titulaire de réaliser à ses frais tous travaux de mise en conformité de ses locaux

Le titulaire a le devoir d'informer sans délai l'Administration de toute difficulté dans l'application de ces mesures, de fuite ou de suspicion de fuite d'informations sensibles qu'il rencontre ou constate

II. Exigences applicables

1- Le Prestataire doit désigner parmi son personnel un correspondant sécurité pour toute la durée de la prestation.

Ce correspondant est notamment :

- L'interlocuteur privilégié de l'ANTS pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées suite à des incidents de sécurité opérationnels
- Le chargé du maintien et de la mise en application du PAS

Ce correspondant doit être joignable aux horaires convenus dans le cadre contractuel. Tout remplacement de ce correspondant doit être notifié à l'ANTS préalablement à son entrée en vigueur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son

indisponibilité.

Il est impératif de préciser la fonction de ce correspondant, responsable de la mise en œuvre et du respect du PAS (le nom et les coordonnées seront fournis dans l'annuaire de la prestation, ses rôles et missions seront détaillés dans le PAS).

Un engagement de devoir d'alerte en cas de changement de responsable est attendu.

2- Le Prestataire doit aborder les aspects sécurité dans le cadre de la gouvernance de la prestation.

Le PAS doit décrire les points suivants :

- Les instances de pilotage de la prestation dans lesquelles la sécurité pourra être abordée
- La fréquence à laquelle la sécurité sera abordée (au minimum trimestrielle)
- Les acteurs sécurité du Prestataire et de l'ANTS y participant

Le PAS doit être validé par l'ANTS au démarrage de la prestation.

3- Les lieux où sont effectuées les prestations doivent être clairement précisés. Les prestations réalisées pour France Titres doivent impérativement se dérouler en France.

4- En cas d'arrêt de la prestation (fin de contrat ou activation de la clause de réversibilité par exemple), pendant toute la durée de la phase de transfert associée, le Prestataire doit assurer le maintien du niveau de sécurité de la prestation décrit dans les documents contractuels. Pour le respect de certaines exigences légales, les exigences liées à la conservation des traces et détaillées dans le PAS sont toujours applicables après l'arrêt de la prestation.

Le Prestataire s'engage à restituer et détruire les données de l'ANTS en fin de prestation. Il dispose pour cela d'une procédure décrivant :

- Les modalités et délais de restitution des données
- La destruction des données présentes sur tous les environnements (production, pré-production, qualification, développement...)
- La destruction des données présentes sur des supports de sauvegardes, même si ceux-ci sont mutualisés.
- Le Prestataire doit informer l'ANTS sur le délai de destruction effective de ces données.
- Le Prestataire doit fournir un rapport de destruction qui mentionne au minimum :

Le succès ou l'échec de l'opération

Les algorithmes ou la méthode utilisée pour la destruction.

Cette exigence reste valable jusqu'à la destruction effective des données (exemple : journaux d'événements, données fiscales...).

5- Des indicateurs Sécurités seront fournis par le Prestataire au client.

Le format de livraison (portail dédié du Prestataire, courriel pour des documents PDF, Excel, etc.) sera précisé ainsi que les destinataires de ces indicateurs et la périodicité de mise à jour ou d'envoi.

Exemples d'indicateurs:

- *Nombre d'incidents de sécurité par typologie*
- *Nombre de collaborateurs intervenant sur le périmètre de la prestation ayant des droits administrateurs sur leur poste de travail et non justifié auprès de l'ANTS*
- *Taux de sous-traitants ayant fait l'objet d'un contrat précisant les exigences de sécurité*
- *Taux d'équipement protégé par un antivirus à jour*
- *Taux de patchs urgents et prioritaires non déployés depuis plus de trois mois*
- *Nombre d'audits de sécurité effectués sur la période et résultats*
- *Nombre de revues de compte et des droits d'accès effectuées sur la période et résultats*
- *Taux de conformité des revues de configurations effectuées sur la période*
- *Taux de sensibilisation des utilisateurs (au RGPD, au phishing etc.)*

6- Le Prestataire doit posséder une Politique de Sécurité des Systèmes d'Information qui décrit les principes généraux de sa politique de sécurité des systèmes d'information.

La PSSI du Prestataire doit notamment préciser la gouvernance en matière de sécurité. Elle doit être diffusée au sein de son organisation, revue régulièrement et déclinée d'un point de vue opérationnel.

7- Les rôles, les responsabilités et l'organisation de la chaîne fonctionnelle Sécurité SI du Prestataire doit être précisée au travers d'une note d'organisation interne précisant la mise en œuvre de la PSSI à l'échelle de la structure et fixant la répartition des responsabilités et rôles en matière de sécurité numérique au sein de chaque entité et au niveau local.

Les rôles et responsabilités liés à la sécurité de l'information sont bien définis et attribués à des personnels ayant les compétences requises. Ceux-ci doivent être clairement identifiés et identifiables par le Client.

8- Toute personne (dont sous-traitant et tiers du Prestataire) intervenant au titre de la prestation doit :

- Faire l'objet d'une sensibilisation périodique à la SSI permettant d'acquérir les fondamentaux de sécurité, de connaître ses droits et devoirs en la matière,
- Faire l'objet d'une formation à la SSI adaptée à son rôle et aux technologies qu'elle manipule,
- Faire l'objet d'un contrôle préalable (criblage) avant son entrée en fonction sur le périmètre de l'ANTS,
- Faire l'objet des habilitations nécessaires en fonction du périmètre exploité.

9- Le Client peut, sur simple demande, consulter les compétences des personnels du Prestataire intervenant sur son périmètre.

Il appartient au Prestataire de fournir au Client tous les éléments permettant cette vérification (CV, preuve de formation, etc.).

10- Le Prestataire doit justifier d'un processus associé à la modification ou à l'achèvement des responsabilités liées au contrat de travail de ses intervenants:

- Restitutions des actifs de façon immédiate
- Modification / suppression des droits d'accès de façon immédiate
- Le cas échéant, révocation des habilitations de façon immédiate

En cas de modification ou achèvement des responsabilités d'un intervenant ou de révocation de ses accès / habilitations, l'ANTS est notifiée sans délai.

11- Toute donnée manipulée dans le cadre de la prestation doit faire l'objet d'une classification de sécurité conforme à la classification des données de l'ANTS :

- Des mesures de sécurité spécifiques à chaque niveau de classification doivent être appliquées sur les informations concernées,
- Tout le cycle de vie de l'information doit faire l'objet d'une classification minutieuse afin d'en contrôler la diffusion,
- Les « personnes ayant le besoin d'en connaître », i.e. personnes qui auront potentiellement accès aux données de la prestation, doivent être conscientes de leur éventuelle sensibilité.

A contrario, les intervenants du Prestataire n'accédant pas à des données sensibles utilisées dans le cadre de la prestation ne doivent pas être informés de leur existence.

12- Tous les documents utilisés dans le cadre de la prestation doivent respecter le marquage relatif notamment au niveau de classification des données associées conformément à la politique de l'ANTS.

La sensibilité des données traitées par un système d'information doit être expressément formalisée (par exemple, dans une procédure d'exploitation de la sécurité) et prise en compte.

13- Pour chaque niveau de classification, la procédure de manipulation, le traitement sécurisé, la conservation, la transmission et la destruction, doivent être conformes à la politique en vigueur au

sein de l'ANTS.

Les informations professionnelles doivent être traitées et stockées uniquement sur le matériel et les solutions mis à disposition ou validés par le Service 3SI de l'ANTS ou il convient de prévoir les clauses contractuelles permettant d'apporter les mêmes garanties. Toute utilisation de matériels personnels est proscrite.

14-Le Prestataire s'engage à restituer les données et actifs de l'ANTS si l'ANTS en fait la demande et dans tous les cas à détruire les données ANTS présentes sur ses environnements.

Le Prestataire s'engage à restituer les actifs et détruire les données de l'ANTS en fin de prestation. Il doit disposer pour cela d'une procédure validée par l'ANTS décrivant :

- Les modalités et délais de restitution des données,
- La destruction des données présentes sur tous les environnements (production, pré-production, qualification, développement, etc.),
- La destruction des données présentes sur des supports de sauvegardes, même si ceux-ci sont mutualisés,
- Pour les données confidentielles et secrètes, la destruction logique est effectuée en utilisant des algorithmes et un nombre de passes suffisant pour que les données soient rendues irrécupérables par des moyens communs (le nombre de passes et les algorithmes à utiliser seront précisés et/ ou validés par le Client).

Le Prestataire doit informer l'ANTS sur le délai de destruction effective de ces données.

Le Prestataire doit fournir un rapport de destruction qui mentionne au minimum :

- Le succès ou l'échec de l'opération,
- Les algorithmes ou la méthode utilisée pour la destruction.

15-Les supports amovibles autorisés sur le périmètre de la prestation doivent être définis avec le Service 3SI de l'ANTS.

Par défaut, le transfert physique de support est interdit par l'ANTS.

Le cas échéant, préciser les modalités de transfert physique des supports. Tout transfert doit être tracé.

16-L'accès à toute ressource non publique nécessite une identification et une authentification individuelle de l'utilisateur.

Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes du besoin d'en connaître et du moindre privilège.

Dans certains cas, un système d'authentification forte devra/pourra être mis en place (exemple: par carte).

Les demandes liées aux accès du personnel du Prestataire au SI de l'ANTS (création, modification, suppression) doivent être centralisées :

- Le Prestataire doit tenir à jour un registre de son personnel intervenant dans le cadre de la prestation,
- Le Prestataire suivra la procédure d'accès au SI de l'ANTS pour toute demande d'accès ou de modification de droits,
- Tout personnel du Prestataire qui ne figure pas sur le registre ne disposera pas d'un compte d'accès au SI,
- Les comptes (identifiants et mots de passe) fournis sont des comptes individuels, nominatifs, non transférables à un tiers, même s'il s'agit d'un collaborateur du Prestataire,
- Si un compte fonctionnel générique est indispensable au fonctionnement d'un service, des

mécanismes supplémentaires de traçabilité sont mis en place de sorte que des contrôles réguliers puissent être faits sur les actions réalisées.

Les mots de passe de ce type de compte doivent être renouvelés tous les 6 mois et à chaque départ d'un utilisateur ayant eu accès au compte générique concerné.

Le Prestataire assurera la réalisation de revues périodiques des comptes d'accès aux ressources informatiques (serveurs, postes de travail, applications) de l'ANTS utilisées dans le cadre de la prestation. La périodicité de ces revues doit être *a minima* d'une fois par an.

17-Tout personnel du Prestataire doit, quant à la confidentialité des éléments d'authentification les concernant, respecter les bonnes pratiques suivantes :

- Ne pas écrire ses identifiants,
- Ne pas partager ses identifiants,
- Utiliser un coffre-fort de mots de passe.

18-Les postes de travail fournis à l'utilisateur par l'ANTS ou le Prestataire, doivent être gérés et configurés sous leur responsabilité respective. La connexion de tout équipement non maîtrisé, non administré ou non mis à jour par l'ANTS ou le Prestataire sur le périmètre exploité est totalement interdite et peut faire l'objet de poursuites.

19-Une procédure de transfert de l'information doit être appliquée.

Toute donnée à caractère confidentiel ou classifié doit être chiffrée avant transmission informatique (chiffrement du flux ou de la donnée elle-même).

Des accords traitant du transfert sécurisé de l'information entre l'ANTS et le Prestataire sont signés. Par défaut, aucune donnée relative à la prestation ne doit transiter sur un SI tiers non maîtrisé (ex: Cloud) sans autorisation explicite de l'ANTS. Les transferts automatiques d'informations avec des tiers sont soumis à validation de l'ANTS.

Tout incident lié à la sécurité de l'information (ex: perte de données) doit être identifié et documenté.

20-Le Prestataire s'engage à faire signer un engagement individuel de confidentialité (EIC) à ses salariés ou toute personne intervenant pour son compte dans le cadre de la prestation et à en transmettre une copie à l'ANTS.

21-Toute prestation pour l'ANTS doit se conformer à minima aux exigences du présent PAS, au RGS et à la PGSN du MI.

22-Des audits indépendants peuvent être régulièrement conduits pour veiller à la pérennité de l'applicabilité, de l'adéquation et de l'efficacité de l'approche du Prestataire en matière de management de la sécurité de l'information.

Auto-contrôle:

Le Prestataire doit effectuer des autocontrôles de conformité aux exigences du présent PAS pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

Pour ce qui concerne la partie « Développement », le Prestataire doit se conformer au guide de développement sécurisé et fournir à l'ANTS, à chaque livraison de code, un scan type SonarQube et un scan de validité des librairies utilisées afin de garantir l'absence de vulnérabilités OWASP dans le code.

En cas de vulnérabilités critiques présentes dans le code, et notamment en cas de vulnérabilité du TOP 10 OWASP, la livraison du code pourra être refusée. Le cas échéant, les vulnérabilités critiques devront impérativement être corrigée lors de la livraison suivante.

Les vulnérabilités majeures pourront faire l'objet d'une dérogation temporaire afin de permettre la recette, mais devront être corrigées sous un délai de 1 à 2 mois.

Il doit fournir et présenter trimestriellement à l'ANTS le tableau de bord des indicateurs sécurité formalisant le résultat de ces autocontrôles.

Contrôle de l'ANTS:

Le Prestataire s'engage à autoriser l'ANTS à réaliser des contrôles de sécurité, de type « scan de vulnérabilités » ou « test d'intrusion informatique » par exemple sur le SI du Titulaire. Sont entendus notamment que :

- Le rapport sera fourni à l'ANTS,
- Le Prestataire s'engage à collaborer de bonne foi avec l'ANTS,
- Le coût des contrôles est supporté par l'ANTS. Toutefois, le coût induit par la participation d'intervenants du Prestataire aux contrôles reste à la charge de celui-ci.

Le Prestataire indique dans le PAS son accord ainsi et peut proposer les modalités d'exécution et le délai de prévenance s'ils ne sont pas précisés au contrat.

23-En cas d'écarts constatés, avec les exigences de sécurité contractuelles, ou en cas de manquement à la sécurité, suite à un audit ou un contrôle, un plan de remédiation devra être formalisé par le Prestataire au plus tard 15 jours après la livraison du rapport.

Ce plan devra être validé conjointement par le Prestataire et l'ANTS.

Le Prestataire devra ensuite régulariser ces écarts ou manquements par l'application du plan de remédiation dans un délai convenu d'un commun accord par les deux parties.