



Règlement de la Consultation

**Acquisition et Tierce Maintenance Applicative (TMA)
d'un outil de GMAO pour l'Institut Mines-Télécom**

25 IMT 019 M

Date et heure limite de réception des offres :

Lundi 14 avril 2025 à 12 heures 00

Délai de rigueur

SOMMAIRE

1.	Objet de la consultation	3
2.	Durée	3
3.	Procédure de passation	3
4.	Allotissement.....	3
5.	PRESTATIONS SUPPLEMENTAIRES EVENTUELLES OBLIGATOIRES.....	4
6.	PRESTATIONS SUPPLEMENTAIRES EVENTUELLES NON OBLIGATOIRES	4
7.	VARIANTES.....	4
8.	Dossier de consultation	4
9.	Envoi des propositions	5
10.	Délai de validité.....	6
11.	Groupements d'opérateurs économiques.....	6
12.	Sous-traitance	7
13.	Présentation du dossier de candidature	7
14.	Présentation du dossier d'offre.....	8
15.	Attribution du marché	8
16.	Critères d'attribution et choix de l'offre	9
17.	renseignements complémentaires.....	10
18.	Litiges et différends	10

ANNEXE 1 AU REGLEMENT DE CONSULTATION

11

Chapitre 1 – PRESentATION DETAILLEE DE LA SOLUTION	11
Chapitre 2 – PRESENTATION DES ASPECTS TECHNIQUES ET DE SECURITE DE LA SOLUTION PROPOSEE	11
CHAPITRE 3 - Engagements de services plan de qualité des services récurrents (PQSR), le plan de réversibilité et le plan d'assurance qualité (PAQ)	12
Chapitre 4 – Equipe pressentie pour l'exécution des prestations.....	12
Chapitre 5 – PLANNING ET METHODOLOGIE PROPOSEES.....	12
CHAPITRE 6 - sécurité de l'information – questionnaire d'homologation.....	12

1. OBJET DE LA CONSULTATION

Objet des fournitures : Acquisition et Tierce Maintenance Applicative d'une solution de Gestion de Maintenance Assistée par Ordinateur (GMAO) pour l'Institut Mines-Télécom et prestations associées.

Le marché comprend :

- une partie forfaitaire (mission de base)
- et, une partie exécutée au fur et à mesure de l'émission de bons de commande pour des prestations complémentaires en application des articles R2362-2 et R 2162-13 à R 2162-14 du Code de la commande publique sans minimum mais avec un montant maximum de 100 000 € HT pour toute la durée du marché.

2. DURÉE

Durée initiale de cet accord-cadre : 36 mois

La durée d'exécution de l'accord-cadre commence à courir à partir de la notification.

Le présent marché comprend une reconduction tacite d'un an.

A l'issue de la dernière reconduction, plus aucune nouvelle commande ne pourra être réalisée en exécution de cet accord-cadre.

Si l'acheteur ne souhaite pas reconduire l'accord-cadre, il doit prendre une décision expresse de non-reconduction, qu'il notifie au titulaire au plus tard 60 jours calendaires avant la date d'échéance de l'accord-cadre initial ou d'une reconduction ultérieure.

Le titulaire ne peut s'opposer à la non-reconduction de l'accord-cadre.

3. PROCÉDURE DE PASSATION

Conformément aux articles R. 2124-2 et R. 2161-2 à R. 2161-5 du code de la commande publique, le marché est passé par appel d'offres ouvert.

Conformément à l'article R. 2162-2 du code de la commande publique, l'accord-cadre mono-attributaire sera exécuté par l'émission de bons de commande dans les conditions fixées aux articles R. 2162-13 et R. 2162-14 du même code.

Nomenclature CPV pertinente :

48421000-5 : Logiciels de gestion des installations (Code CPV principal)

4. ALLOTISSEMENT

L'acheteur décide de ne pas allotir l'accord-cadre initial pour les raisons suivantes :
Le marché ne comporte pas de prestations distinctes.

5. PRESTATIONS SUPPLEMENTAIRES EVENTUELLES OBLIGATOIRES

L'IMT demande au titulaire de proposer, dans son offre, des prestations supplémentaires, qu'il se réserve le droit de commander ou non lors de la signature du marché.

Le prestataire proposera en prestations supplémentaires obligatoires pour l'ensemble des entités:

- Gestion des pièces de rechange (PSE 1)
- Repérage des équipements par QR Code (PSE 2)
- Interfaçage complet avec les outils de ticketing IMT : GLPI & OTRS (PSE 3).

6. PRESTATIONS SUPPLEMENTAIRES EVENTUELLES NON OBLIGATOIRES

Le prestataire pourra proposer, un hébergement externe de la solution de GMAO. Dans ce cas Il devra détailler les modalités : Lieu, prestataire (hébergeur), infrastructure, technologie, niveau de sécurité...

7. VARIANTES

Les candidats pourront présenter une variante portant sur ***la présentation de la décomposition du prix global et forfaitaire de la mission de base et la prestation à bons de commande « Acquisition de licences »***.

La variante éventuellement proposée ne devra pas modifier les prestations demandées dans la mission de base, mais pourra uniquement ventiler différemment la présentation du coût global et forfaitaire associé. S'agissant de l'acquisition de licences, le candidat pourra proposer un coût dégressif en fonction du nombre de licences commandées.

La variante pourra être présentée sans l'offre de base.

8. DOSSIER DE CONSULTATION

Vous pouvez consulter les documents en ligne à l'adresse suivante : www.marches-publics.gouv.fr/

Le dossier de consultation comprend les éléments suivants :

- L'acte d'engagement (AE) et son annexe financière (bordereau de prix/DQE)
- Le présent Règlement Consultation (RC) et son annexe (présentation du mémoire technique)
- Le Cahier des Clauses Administratives Particulières (CCAP)
- Le Cahier des Clauses Techniques Particulières (CCTP) et ses annexes 1 et 2.

L'acheteur se réserve le droit d'apporter des modifications de détail au dossier de consultation. Ces modifications devront être reçues par les candidats au plus tard 7 jours calendaires avant la date limite de réception des offres. Les candidats devront alors répondre sur la base du dossier modifié sans pouvoir élever aucune réclamation à ce sujet.

Les renseignements complémentaires sur les documents de la consultation seront envoyés aux opérateurs économiques 6 jours calendaires au plus tard avant la date limite fixée pour la réception des offres, pour autant qu'ils en aient fait la demande 7 jours calendaires avant la date limite fixée pour la réception des offres.

Si un complément d'informations, nécessaire à l'élaboration de l'offre n'est pas fourni dans les délais prévus ci-dessus, ou si des modifications importantes sont apportées aux documents de l'accord-cadre, le délai de réception des offres sera prolongé de manière proportionnée à l'importance des informations demandées ou des modifications apportées.

9. ENVOI DES PROPOSITIONS

Les plis doivent être remis au plus tard à la date et l'heure mentionnées en page de garde du présent document. Les plis déposés postérieurement seront considérés comme étant hors délai.

Conformément aux articles R.2132-7 et R.2132-8 du Code de la commande publique, les candidats devront obligatoirement transmettre leurs propositions de manière électronique.

Transmission par voie électronique

Les candidats devront tenir compte des indications suivantes, afin de garantir au mieux le bon déroulement de cette procédure dématérialisée.

La plate-forme de dématérialisation à utiliser pour la remise des offres est la suivante : www.marches-publics.gouv.fr/

La liste des formats de fichiers acceptés est la suivante :

- Portable Document Format (Adobe .pdf),
- Rich Text Format (.rtf),
- Compressés (exemples d'extensions : .zip, .rar),
- Applications bureautiques (exemples d'extensions : .doc, .xls, .pwt, .pub, .mdb),
- Multimédias (exemples d'extensions : gif, .jpg, .png).

Les documents nécessitant une signature, transmis par voie dématérialisée, sont de préférence signés individuellement par le candidat au moyen d'un certificat de signature électronique conforme au format XAdES, CAdES ou PAdES. Les certificats de type RGS peuvent encore être utilisés après le 1er octobre 2018 pour le temps de leur validité.

Le cas échéant, les documents transmis par voie électronique pourront être rematérialisés après l'ouverture des plis pour signature. Les candidats sont informés que les pièces non signées électroniquement pourront être rematérialisées et signées manuscritement après l'attribution. Dans cette hypothèse, l'attributaire désigné s'engage à signer l'acte d'engagement et toutes autres pièces éventuelles conformément à l'offre remise ou négociée.

Les frais d'accès au réseau et de recours à la signature électronique sont à la charge de chaque candidat.

Copie de sauvegarde

Parallèlement à l'envoi électronique, le candidat peut effectuer, à titre de copie de sauvegarde, une transmission supplémentaire sur support physique électronique (CD-Rom, DVD-Rom, clé USB) ou sur support papier.

Ce pli scellé comporte obligatoirement le numéro du marché, le nom du candidat et la mention : « copie de sauvegarde ».

Cette copie est envoyée par pli recommandé avec demande d'avis de réception ou remise en main propre contre récépissé à l'adresse suivante :

**Institut Mines-Télécom
Direction générale - Direction juridique
19 Place Marguerite Perey,
91120 Palaiseau**

10. DÉLAI DE VALIDITÉ

Le candidat reste lié par son offre pendant un délai de 90 jours calendaires, à compter de la date limite de présentation des offres.

11. GROUPEMENTS D'OPÉRATEURS ÉCONOMIQUES

Conformément à l'article R. 2142-19 du code de la commande publique, les groupements d'opérateurs économiques peuvent participer à la présente consultation.

Lors de la remise de la candidature et de l'offre, la forme juridique du groupement est laissée à la libre appréciation des candidats.

Le groupement pourra prendre la forme soit d'un groupement conjoint, soit d'un groupement solidaire.

Quelle que soit la forme juridique du groupement retenue par les candidats, la composition du groupement devra être détaillée et l'un des opérateurs économiques membre du groupement sera désigné comme mandataire. Ce mandataire représentera l'ensemble des membres du groupement vis-à-vis de l'acheteur et coordonnera les prestations des membres du groupement.

Un même opérateur économique ne peut pas être mandataire de plus d'un groupement pour un même marché public.

Conformément aux dispositions de l'article R. 2142-26 du code de la commande publique, la composition du groupement ne pourra pas être modifiée entre la date de remise des candidatures et la date de signature du marché.

Il pourra cependant être dérogé à ce principe en cas d'opération de restructuration de société, notamment de rachat, de fusion ou d'acquisition touchant l'un des membres du groupement ou, si le groupement apporte la preuve qu'un de ses membres se trouve dans l'impossibilité d'accomplir sa tâche pour des raisons qui ne sont pas de son fait. Le groupement pourra alors demander à l'acheteur l'autorisation de continuer à participer à la procédure de passation en proposant, le cas échéant, à l'acceptation de l'acheteur, un ou plusieurs nouveaux membres du groupement, sous-traitants ou entreprises liées.

L'acheteur se prononcera sur la recevabilité de cette demande après examen de la capacité de l'ensemble des membres du groupement ainsi transformé et, le cas échéant, des sous-traitants et entreprises liées présentées à son acceptation, au regard des conditions de participation qu'il a définies.

Les opérateurs économiques ne sont pas autorisés à candidater en agissant à la fois en qualité de candidat individuel et de membre d'un groupement. Les opérateurs économiques ne sont pas autorisés à candidater en qualité de membres de plusieurs groupements.

12. SOUS-TRAITANCE

Le soumissionnaire présente dans son offre les sous-traitants dont l'intervention est envisagée, s'ils sont connus.

Pour chaque sous-traitant présenté dans l'offre, le soumissionnaire joindra :

- les pièces permettant de justifier des capacités techniques, professionnelles et financières du sous-traitant lorsque le candidat ou l'un des membres du groupement candidat s'appuie sur la ou les capacités du sous-traitant proposé. Le candidat joindra à cet égard la preuve qu'il disposera des capacités de l'opérateur économique pour l'exécution du marché;
- une déclaration indiquant que le sous-traitant ne tombe pas sous le coup d'une interdiction de soumissionner aux marchés publics;
- le formulaire DC4 (déclaration de sous-traitance) dans sa dernière mise à jour dûment complété et signé.

13. PRÉSENTATION DU DOSSIER DE CANDIDATURE

Dans le cadre de sa candidature, le candidat devra produire les documents suivants.

Si ceux-ci ne sont pas remis en français, une traduction des documents devra être jointe au dossier de candidature.

Le candidat peut présenter sa candidature sous forme d'un document unique de marché européen (DUME), en lieu et place des formulaires DC1 et DC2. En cas de groupement d'opérateurs économiques, chacun des membres du groupement fournira un formulaire DUME complété.

Les capacités professionnelles, techniques et financières du candidat seront analysées à partir des critères listés ci-dessous. Lorsqu'un niveau minimum est exigé pour un critère, le candidat doit fournir les preuves des minimaux demandés ou toute autre forme de preuve équivalente.

N°	Capacité économique et financière du candidat
1	Déclaration concernant le chiffre d'affaires global du candidat et, le cas échéant, le chiffre d'affaires du domaine d'activité faisant l'objet du marché public, portant au maximum sur les trois derniers exercices disponibles en fonction de la date de création de l'entreprise ou du début d'activité de l'opérateur économique, dans la mesure où les informations sur ces chiffres d'affaires sont disponibles.

N°	Capacité technique et professionnelle du candidat
1	Une déclaration indiquant les effectifs moyens annuels du candidat et l'importance du personnel d'encadrement pour chacune des trois dernières années.
2	Une liste des principales livraisons effectuées ou des principaux services fournis au cours des trois dernières années, indiquant le montant, la date et le destinataire public ou privé. Les livraisons et les prestations de services sont prouvées par des attestations du destinataire ou, à défaut, par une déclaration de l'opérateur économique.

Conformément aux dispositions de l'article R 2143-13 du Code de la commande publique, les candidats ne sont pas tenus de fournir les documents justificatifs et moyens de preuve que l'acheteur peut obtenir directement par le biais d'un système électronique de mise à disposition d'informations administré par un organisme officiel ou d'un espace de stockage numérique, à condition que figure dans le dossier de candidature toutes les informations nécessaires à la consultation de ce système ou de cet espace et que l'accès à ceux-ci soit gratuit.

Les candidats sont invités à utiliser le coffre-fort électronique disponible gratuitement depuis leur compte sur <https://declarants.e-attestations.com>

14. PRÉSENTATION DU DOSSIER D'OFFRE

Dans le cadre de son offre, le candidat devra produire les documents suivants.

Si ceux-ci ne sont pas remis en français, une traduction des documents devra être jointe au dossier d'offre.

N°	Description
1	L'acte d'engagement Le document doit être dûment rempli, daté par la personne habilitée à engager la société. Le candidat auquel il est envisagé d'attribuer le marché public sera tenu de signer l'acte d'engagement. Toutefois, le candidat peut choisir de le signer dès le dépôt de sa candidature ou de son offre.
2	Le bordereau de prix et le DQE Le document doit être dûment rempli par la personne habilitée à engager la société. Les prix doivent toujours être exprimés en euro.
3	Le relevé d'identité bancaire
5	Le mémoire technique présenté selon l'annexe 1 au présent règlement de consultation (cadre du mémoire technique)

Aucune signature n'est requise pour les documents de la candidature et de l'offre lors du dépôt du pli (à l'exception de l'habilitation du mandataire par ses co-traitants, mais qui ne sera demandée, le cas échéant, qu'en fin de procédure si l'attributaire est constitué en groupement).

15. ATTRIBUTION DU MARCHÉ

Au terme de la procédure, l'acheteur demandera à l'opérateur économique ou au mandataire du groupement d'opérateurs auquel il est envisagé d'attribuer l'accord-cadre de lui retourner :

- L'acte d'engagement dûment rempli, daté et signé par la personne habilitée à engager la société.
- Les attestations d'assurance reprises dans le CCAP
- Les documents justificatifs visés aux articles R. 2143-6 à R. 2143-10 du Code de la commande publique. Le cas échéant, il sera fait application des articles R. 2143-13 et R. 2143-15 du Code de la commande publique.

Lors de la conclusion de l'accord-cadre et tous les 6 mois jusqu'à la fin de celui-ci, il sera demandé au titulaire de l'accord-cadre de fournir une attestation de vigilance afin de prouver qu'il respecte les règles applicables en matière de lutte contre le travail dissimulé.

16. CRITÈRES D'ATTRIBUTION ET CHOIX DE L'OFFRE

L'acheteur attribue l'accord-cadre au soumissionnaire ayant présenté l'offre économiquement la plus avantageuse en se fondant sur une pluralité de critères.

Les critères listés ci-dessous s'appliquent pour l'attribution de l'accord-cadre :

- **Prix des prestations: 40 %**
 - Prix de la mission de base (forfaitaire) (70 points)
 - Prix des prestations à bons de commande (30 points)
- **Valeur technique appréciée sur la base du mémoire technique : 60 %**
 - Equipe/moyens humains proposés (CV/Expérience) et notamment composition et expériences/références de l'équipe proposée dans le domaine objet du marché (15 points)
 - Contenu fonctionnel de la solution proposée (35 points)
 - Contenu technique et de sécurité de la solution proposée (20 points)
 - Planning et méthodologie d'implémentation du projet et de la TMA proposés (15 points)
 - Engagements de services plan de qualité des services récurrents (PQSR), le plan de réversibilité et le plan d'assurance qualité (PAQ) (15 points)

Une certaine valeur a été attribuée à chaque critère. Sur la base de l'évaluation de tous ces critères, tenant compte de la valeur attribuée à chacun, l'accord-cadre sera attribué au candidat présentant l'offre régulière économiquement la plus avantageuse du point de vue de l'acheteur.

Si une offre lui paraît anormalement basse, l'acheteur demandera au soumissionnaire d'apporter les précisions et justifications permettant de démontrer que l'offre présentée n'est pas anormalement basse, en application des articles L. 2152-5 à L. 2152-6 et R. 2152-3 à R. 2152-5 du code de la commande publique.

Si les éléments produits par le soumissionnaire ne permettent pas de justifier de manière satisfaisante le bas niveau des prix proposés ou si le soumissionnaire se trouve dans l'un des cas précisés aux articles R. 2152-4 ou R. 2152-5 du code de la commande publique, son offre est rejetée.

L'analyse du critère prix se fera sur la base du détail quantitatif estimatif (DQE). Il est à noter que les prix indiqués dans le DQE devront être rigoureusement identiques à ceux indiqués dans le

bordereau de prix unitaires (BPU). Si des discordances étaient constatées, l'acheteur pourra rejeter l'offre du candidat.

17. RENSEIGNEMENTS COMPLÉMENTAIRES

Pour obtenir tous les renseignements complémentaires qui leur seraient nécessaires pendant la consultation, les candidats devront faire parvenir leur demande par l'intermédiaire du profil d'acheteur de l'acheteur, à l'adresse suivante : www.marches-publics.gouv.fr/.

18. LITIGES ET DIFFÉRENDS

Les différends et litiges se règlent selon les dispositions de l'article 55 du CCAG des marchés publics de Techniques de l'Information et de la Communication.

En cas de litige, les coordonnées de l'instance chargée des procédures de recours sont les suivantes :

Tribunal Administratif de Versailles

Tél. : 01 39 20 54 00

Fax : 01 39 20 54 87

Email : greffe.ta-versailles@juradm.fr

Annexe 1 au Règlement de consultation

Le « Mémoire technique » est destiné à recueillir les éléments de l'offre technique du candidat en support de sa réponse à la consultation. Les critères de sélection des offres sont pondérés sur la qualité des réponses aux questions posées sur les différents chapitres. Ce document constitue aussi l'ossature des prestations et services, objets de l'engagement du titulaire pendant toute la durée du contrat. **L'attention du candidat est attirée sur le fait que le cadre de réponse est un document particulier constitutif du marché et que toutes les affirmations et engagements, qui y sont consignés, sont contractuels et deviennent exécutoires.**

Le candidat répond impérativement à toutes les questions posées en explicitant de façon concise ses réponses. Le cadre de réponse du mémoire technique est composé des chapitres 1 à 6.

CHAPITRE 1 – PRESENTATION DETAILLEE DE LA SOLUTION

Le candidat présentera la solution (outil) proposée et notamment :

- Description de l'ensemble des fonctionnalités de la solution, front-office et back-office
- la gestion de la structure organisationnelle,
- la gestion du préventif,
- la gestion du curatif,
- la gestion des référentiels,
- la gestion en mode déconnecté,
- la gestion avec QR Code,
- le lien avec les outils de ticketing GLPI & OTRS,
- les exigences fonctionnelles générales,
- la reprise des données et les interfaces – API

CHAPITRE 2 – PRESENTATION DES ASPECTS TECHNIQUES ET DE SECURITE DE LA SOLUTION PROPOSEE

Le candidat présentera les aspects techniques et de sécurité de la solution proposée et notamment :

- Les modalités d'hébergement
- L'architecture applicative (Software),
- La souplesse d'évolution du produit,
- Les interfaces,
- L'architecture technique,
- Les exigences réseaux des applications,
- La performance et qualité,
- La prise en compte du RGPD et des mesures de sécurité des systèmes d'information (SSI)
- La réversibilité.

CHAPITRE 3 - ENGAGEMENTS DE SERVICES PLAN DE QUALITÉ DES SERVICES RÉCURRENTS (PQSR), LE PLAN DE RÉVERSIBILITÉ ET LE PLAN D'ASSURANCE QUALITÉ (PAQ)

Le candidat présentera sa proposition en matière :

- D'engagements de services plan de qualité des services récurrents (PQSR), le plan de réversibilité et le plan d'assurance qualité (PAQ)

CHAPITRE 4 – EQUIPE PRESSENTIE POUR L'EXÉCUTION DES PRESTATIONS

Le candidat présentera le détail de son organisation interne répondant directement aux besoins exprimés, sa capacité et son expérience en regard des prestations demandées. Le candidat pourra fournir des références de clients pour lesquels il opère un type de prestations identique aux besoins exprimés.

Le candidat présentera les CV détaillés de l'équipe d'intervenants mobilisés ainsi que la description de leur expérience acquise et leur rôle respectif dans l'organisation proposée pour remplir les besoins exprimés.

CHAPITRE 5 – PLANNING ET METHODOLOGIE PROPOSEES

Le candidat fournira une note méthodologique présentant notamment :

- Le Planning et la méthodologie d'implémentation du projet (BUILD) proposé
- La méthodologie de la phase de TMA (Tierce Maintenance Applicative)(RUN)
- Les modalités de formation des utilisateurs
- La comitologie pour les phases de projet (BUILD) et de TMA (RUN)

CHAPITRE 6 - SÉCURITÉ DE L'INFORMATION – QUESTIONNAIRE D'HOMOLOGATION.

Afin de pouvoir rendre homologable l'application dans le système d'information de l'IMT (voir décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics), le titulaire remplira le questionnaire de sécurité.

Annexe II **Sécurité de l'information**

Nom de la mesure	Référentiel	Type	Catégorie	Description
------------------	-------------	------	-----------	-------------

Fixer et/ou identifier les exigences de sécurité incombant aux prestataires	ANSSI	Indispensable	Gouvernance	<p>En cas de recours à des prestataires, fixer, dès les clauses contractuelles, les exigences de sécurité à respecter. Dans le cas où ces exigences ne peuvent pas être fixées a priori (ex. produit obtenu sur étagère), identifier l'ensemble des exigences de sécurité que s'engagent à respecter les prestataires. Cette mesure permet d'éclairer la sélection des prestataires en fonction des garanties de sécurité que ces derniers s'engagent à respecter.</p> <p>Lister l'ensemble des données à protéger en priorité (ex. données sensibles) et identifier leur localisation (technique et géographique). Cette mesure permet de connaître les données les plus sensibles à protéger, d'évaluer l'impact de leur compromission et d'identifier, de besoin, des mesures de sécurité spécifiques à mettre en œuvre en vue de les protéger.</p>
Identifier les données importantes à protéger	ANSSI	Indispensable	Gouvernance	<p>Créer et tenir à jour un registre des équipements et des applicatifs (ex. serveurs de base de données, annuaires, pare-feu, systèmes de gestion de contenu) participant au fonctionnement du service numérique. Cette mesure est nécessaire afin d'assurer la gestion des mises à jour fonctionnelles et de sécurité du service, indispensables au maintien de la sécurité du service.</p>
Disposer d'une liste à jour des équipements et des applicatifs contribuant au fonctionnement du service numérique	ANSSI	Indispensable	Gouvernance	<p>Configurer le service en vue de limiter, au strict nécessaire, ses interconnexions avec d'autres systèmes d'information et tenir une cartographie à jour de l'ensemble de ces interconnexions. Cette mesure permet de réduire le risque de propagation d'une cyberattaque de ces systèmes vers le service et inversement.</p>
Limitier et connaître les interconnexions entre le service numérique et d'autres systèmes d'information	ANSSI	Indispensable	Gouvernance	<p>Disposer et tenir à jour une liste des comptes disposant d'un accès administrateur au service, les personnes associées et la nature de leur(s) accès. Sont concernés par cette mesure les administrateurs techniques (ex. accès à la configuration de l'hébergement du service) et les administrateurs métiers (ex. agent public ayant un droit de modification des informations affichées sur le service). Cette mesure permet de gérer la liste des comptes disposant d'un accès privilégié en vue d'en limiter le</p>
Disposer d'une liste à jour des comptes disposant d'un accès privilégié au service	ANSSI	Indispensable	Gouvernance	

nombre au strict nécessaire et ainsi réduire le risque que des comptes non nécessaires soient détournés par un acteur malveillant.

Héberger le service numérique et les données au sein de l'Union européenne	ANSSI	Recommandée	Gouvernance	Privilégier le recours à un hébergeur proposant la localisation au sein de l'Union européenne du service numérique et des données. Cette mesure vise à renforcer la protection des données grâce aux garanties offertes par la réglementation européenne et à faciliter les actions de remédiation et d'investigation en cas d'incident de sécurité.
Réaliser un test d'intrusion ou une campagne de recherche de bug	ANSSI	Indispensable	Gouvernance	Faire réaliser un test d'intrusion et/ou une campagne de recherche de bug (bug bounty) du service, par un prestataire ou par un service compétent. Cette mesure permet d'identifier des vulnérabilités du service en vue de les corriger et ainsi renforcer sa sécurité.
Procéder à des vérifications techniques automatiques de la sécurité du service	ANSSI	Indispensable	Gouvernance	Lors du développement du service et, autant que possible, dans le cas de l'achat d'un service sur étagère, procéder à des tests techniques automatiques de la sécurité du service. Cette mesure permet de vérifier rapidement l'existence de vulnérabilités non corrigées parmi les vulnérabilités les plus connues.
Sensibiliser les administrateurs aux consignes de sécurité liées à l'utilisation du service	ANSSI	Indispensable	Gouvernance	Diffuser les mesures de sécurité du service devant être suivies par les administrateurs technique et métier (ex. agents publics chargés de mettre à jour le contenu du service ou accédant aux données de ce dernier). Fixer, de besoin, des consignes spécifiques additionnelles relatives à leur utilisation du service. Sensibiliser régulièrement les administrateurs aux bonnes pratiques de sécurité informatique. Cette mesure vise à impliquer les agents dans la mise en œuvre des mesures prévues pour sécuriser le service et à accroître leur vigilance et leurs réflexes en cas de situation à risque.

Rendre public une procédure permettant de signaler un problème de sécurité	ANSSI	Recommandée	Gouvernance	<p>Fournir publiquement une procédure permettant à une personne ou à une entité de signaler un problème de sécurité concernant le service numérique. Cette procédure doit préciser les conditions dans lesquelles un problème de sécurité peut être identifié et signalé et fournir un moyen non nominatif de contacter l'équipe en charge du service ou de sa sécurité (ex. email, formulaire de contact). Cette mesure facilite l'identification et le traitement de problèmes de sécurité concernant le service.</p> <p>Créer des comptes d'administration technique et/ou métier, aux seules personnes ayant besoin de disposer de ces accès. Cette mesure permet de limiter le nombre de comptes disposant de privilèges susceptibles d'être usurpés à des fins malveillantes. Cette mesure réduit la « surface d'attaque » du service.</p> <p>Lors de la création ou de la modification des privilèges associés à un compte d'administration, limiter ces derniers aux seuls privilèges nécessaires au rôle d'administration visé (ex. limiter aux seules fonctions d'administration de la base de données). Cette mesure permet de réduire la capacité d'action d'un acteur malveillant qui parviendrait à usurper un compte administrateur et ainsi de limiter sa capacité de nuisance.</p> <p>Créer des comptes d'accès d'administration différents dotés de privilèges distincts, pour les personnes devant assurer plusieurs rôles d'administration, que ceux-ci soit techniques (ex. développement, hébergement) et/ou métiers (ex. création de contenus). Cette mesure permet de limiter la capacité d'action d'acteurs malveillants qui parviendraient à usurper un compte d'administration.</p> <p>Créer des comptes d'accès distincts aux personnes à la fois administratrices et utilisatrices du service. Cette mesure permet de réduire le risque d'accès illicite à un compte utilisateur qui permettrait d'accéder également à un compte d'administration aux privilèges élevés.</p>
Limiter au strict nécessaire le nombre de personnes disposant d'un accès administrateur au service numérique	ANSSI	Indispensable	Protection	
Limiter les droits de chaque administrateur au strict nécessaire	ANSSI	Indispensable	Protection	
Dissocier les rôles d'administration entre eux	ANSSI	Indispensable	Protection	
Dissocier les rôles d'administration et des rôles d'utilisation du service	ANSSI	Indispensable	Protection	

Autoriser uniquement la création de comptes d'accès nominatifs associés chacun à une personne	ANSSI	Indispensable	Protection	Demander un nom et un prénom pour toute création de compte administrateur et utilisateur et informer chaque personne que le compte ne peut pas être partagé Cette mesure permet de réduire le risque de diffusion d'identifiants et de mots de passe à des personnes qui n'auraient pas le droit d'accéder au service ou à certaines de ses fonctions. Cette mesure également à la bonne gestion des comptes d'accès au service. Configurer le service en vue de prévoir la suppression régulière des comptes d'accès inactifs, en priorisant la suppression des comptes d'administration. Informer les personnes concernées avant toute suppression de compte. Cette mesure permet d'éviter en priorité que des comptes demeurent actifs sans raison valable, afin de réduire le nombre de comptes susceptibles d'être usurpés par un acteur malveillant.
Mettre en œuvre une procédure de suppression des comptes inactifs	ANSSI	Recommandée	Protection	Fixer des règles de longueur et de complexité des mots de passe lors de la création d'un mot de passe ou de son renouvellement par un utilisateur ou un administrateur. Lorsque cela est possible, configurer le service pour interdire les mots de passe faibles. Cette mesure permet de diminuer le risque de découverte et l'usurpation de mots de passe par des acteurs malveillants, par exemple en testant plusieurs mots de passe sur la base de mots du dictionnaire.
Fixer des contraintes de longueur et de complexité des mots de passe	ANSSI	Indispensable	Protection	Activer l'authentification multifacteur et la rendre obligatoire pour l'accès des administrateurs au service. Proscrire, autant que possible, le recours à un service numérique qui ne prévoirait pas l'authentification multifacteur pour son administration. Cette mesure permet de réduire le risque d'accès illicite aux fonctions d'administration du service par des acteurs malveillants et diminue, d'autant, le risque d'atteinte grave au service.
Activer l'authentification multifacteur pour l'accès des administrateurs au service	ANSSI	Indispensable	Protection	Recommander ou proposer aux administrateurs le recours à une ou plusieurs solutions de gestion de mots de passe sécurisés, permettant de générer des mots de passe aléatoires et robustes et de les enregistrer. Cette mesure permet de faciliter la création de mots de passe différents, longs et
Encourager les administrateurs à utiliser un coffre fort de mots de passe	ANSSI	Indispensable	Protection	

				complexes, distincts pour chaque compte d'accès, sans effort de mémorisation.
Planifier le renouvellement régulier des mots de passe des administrateurs	ANSSI	Recommandée	Protection	Configurer ou recommander à intervalle régulier le renouvellement des mots de passe des comptes d'administration. Cette mesure permet d'éviter qu'un mot de passe ancien ou proche d'un mot de passe déjà utilisé toujours utilisé ne soit découvert et utilisé par un acteur malveillant. Demander aux administrateurs techniques du service de n'administrer ce dernier que depuis un environnement informatique dédié et sécurisé. Le recours à des équipements personnels doit notamment être proscrit. Cette mesure vise à diminuer le risque de compromission des droits d'administration service via des moyens informatiques insuffisamment sécurisés.
Administrer techniquement le service dans des environnements dédiés et sécurisés	ANSSI	Recommandée	Protection	Lors du développement ou de l'achat du service, toujours utiliser une version récente et maintenue à jour par les éditeurs, des applicatifs contribuant au fonctionnement du service (ex. une version récente et à jour d'un système de gestion de contenu (CMS), des dépendances d'une l'application). Cette mesure vise à éviter d'utiliser des versions anciennes, susceptibles de comporter des vulnérabilités connues mais non corrigées ou qui ne seraient plus appelées à faire l'objet de mises à jour de sécurité à l'avenir par l'éditeur.
Utiliser des applicatifs récents et maintenus à jour par leurs éditeurs	ANSSI	Indispensable	Protection	Identifier, tester et installer, sans délai, les mises à jour fonctionnelles et de sécurité des applicatifs et/ou équipement contribuant au fonctionnement et à l'administration du service. Cette mesure vise à renforcer la sécurité du service en permettant de corriger rapidement les failles de sécurité susceptibles de l'affecter.
Disposer d'une politique d'application des mises à jour fonctionnelles et de sécurité du service numérique	ANSSI	Indispensable	Protection	

Installer uniquement les fonctionnalités nécessaires aux finalités du service	ANSSI	Indispensable	Protection	<p>Lors du développement du service ou de l'installation des applicatifs contribuant à son fonctionnement, installer uniquement les fonctionnalités nécessaires et désactiver toutes les fonctionnalités inutiles proposées par défaut. Cette mesure correspond à la règle de la « configuration minimaliste ». Cette mesure permet d'éviter d'installer des fonctionnalités non nécessaires qui pourraient comporter des vulnérabilités non corrigées et servir de vecteurs à une attaque. Cette approche permet de réduire la « surface d'attaque » à savoir l'ensemble des éléments constitutifs d'un service qui pourraient être ciblés par un attaquant.</p> <p>Lors de l'installation d'un applicatif contribuant au fonctionnement du service, restreindre au strict nécessaire ses privilèges - à savoir les droits l'autorisant de mener certaines actions de manière autonome - et ne conserver que les privilèges nécessaires à sa finalité. Cette mesure permet d'éviter que des privilèges non nécessaires accordés à un applicatif ne soient exploités à des fins malveillantes par un attaquant.</p> <p>Formaliser une procédure à suivre en cas d'incident de sécurité sur le service, pouvant inclure des éléments relatifs à la gestion technique de l'incident, la coordination des personnes concernées au sein de l'organisation, la communication aux utilisateurs et aux autres entités potentiellement impactées. Sauvegarder ce document dans un environnement sécurisé, déconnecté du service. Cette mesure permet de préparer l'organisation à réagir de manière rapide et efficace en cas d'incident de sécurité affectant le service et à remédier à la situation.</p> <p>Réaliser à intervalle régulier (ex. une fois par an) un test de la procédure de gestion des incidents de sécurité du service ou de plusieurs services, en impliquant les personnes concernées (ex. vérifier que les coordonnées sont exactes, vérifier la disponibilité des personnes). Cette mesure vise à vérifier que la procédure de gestion des incidents en place fonctionne bien dans la pratique.</p>
Limitier au strict nécessaire les privilèges des applicatifs contribuant au fonctionnement du service	ANSSI	Indispensable	Protection	
Définir une procédure de gestion des incidents de sécurité	ANSSI	Indispensable	Défense	
Tester régulièrement la procédure de gestion des incidents de sécurité	ANSSI	Indispensable	Défense	

Envoyer une notification aux administrateurs et aux utilisateurs à chaque connexion	ANSSI	Recommandée	Défense	<p>Configurer le service afin de proposer l'envoi d'une notification (ex. par email) aux utilisateurs et aux administrateurs, à chaque fois que ceux-ci se connectent. Signaler, si possible, toute tentative de connexion suspecte, par exemple, lorsque la connexion est effectuée depuis un nouvel appareil ou depuis une localisation inhabituelle. Dans le cas de l'achat d'une solution sur étagère, privilégier un service proposant l'envoi de notifications. Cette mesure permet aux utilisateurs et administrateurs d'identifier des tentatives de connexion suspectes et d'empêcher de futures nouvelles tentatives de connexion illégitimes, par exemple, en changeant leur mot de passe.</p> <p>Lors de la configuration du service, activer la journalisation et la centralisation des accès des administrateurs, des utilisateurs et des applicatifs concourant au fonctionnement du service. Cette mesure permet de faciliter la détection d'actions inhabituelles susceptibles d'être malveillantes et d'investiguer a posteriori les causes d'un incident de sécurité, en vue de faciliter sa remédiation.</p> <p>Lors de la configuration du service, activer, si cela est possible, la journalisation et la centralisation des événements de sécurité. A défaut, créer et maintenir à jour un document recensant l'ensemble des événements de sécurité ayant affecté le service et des mesures mises en œuvre pour y remédier. Cette mesure permet de faciliter la détection d'événements de sécurité connus et la résolution des incidents qui en découleraient.</p> <p>Consulter plusieurs sources d'informations sur les vulnérabilités concernant les applicatifs participant au fonctionnement du service ainsi que sur les campagnes de compromission connues (ou campagnes d'attaques informatiques), notamment les alertes de sécurité du CERT-FR. Cette mesure permet d'identifier des vulnérabilités ou risques nouveaux pour le service et de mettre en œuvre les mesures de sécurité permettant d'y faire face, par exemple des mises à jour de sécurité.</p>
Conserver l'historique des accès des administrateurs au service	ANSSI	Recommandée	Défense	
Conserver l'historique de l'ensemble des événements de sécurité sur le service	ANSSI	Indispensable	Défense	
Réaliser une veille régulière des vulnérabilités et des campagnes de compromission	ANSSI	Recommandée	Défense	

Mettre en place une sauvegarde régulière des données dans un environnement non connecté au service numérique	ANSSI	Indispensable	Résilience	<p>Sauvegarder les données traitées par le service, au moins une fois par semaine, dans un environnement sécurisé, déconnecté de ce dernier (ex. dans une autre machine virtuelle chiffrée, sur un ordinateur ou un serveur local déconnecté d'internet). Cette mesure permet une restauration rapide des données, à partir de la dernière sauvegarde des données effectuée, en cas d'incident de sécurité qui conduirait à leur suppression ou les rendrait inaccessibles, par exemple, en cas d'attaque par rançongiciel.</p> <p>Réaliser des tests réguliers des sauvegardes (ex. tous les trois mois) afin de vérifier que celles-ci sont bien réalisées, accessibles et fonctionnelles. Cette mesure permet de vérifier que les sauvegardes effectuées peuvent être utilisées pour restaurer le service et/ou ses données en cas d'incident de sécurité.</p>
Vérifier régulièrement les sauvegardes	ANSSI	Indispensable	Résilience	<p>Configurer le service afin d'activer la déconnexion automatique des sessions des administrateurs et des utilisateurs inactifs après une durée déterminée. Cette mesure vise à limiter le risque d'utilisation, par une personne malveillante, du compte d'un utilisateur, qui aurait laissé son équipement non verrouillé sans surveillance et ne se serait pas déconnecté du service.</p>
Mettre en place la déconnexion automatique des sessions d'accès après une durée déterminée	ANSSI	Recommandée	Protection	<p>Recourir à une ou plusieurs solutions garantissant un haut niveau de disponibilité du service (ex. obligation de redondance de la machine virtuelle et des données). Cette mesure permet d'éviter une interruption du service dépassant quelques minutes.</p>
Recourir à une ou plusieurs solutions garantissant un haut niveau de disponibilité du service	ANSSI	Recommandée	Résilience	<p>Organiser un exercice simulant une crise consécutive à un ou plusieurs incidents de sécurité aux conséquences particulièrement graves pour l'organisation. Cette mesure permet d'entraîner les équipes, d'identifier freins à la gestion efficace d'une crise et de les corriger en vue de se préparer à la survenue d'une crise réelle.</p>
Organiser un exercice de gestion de crise	ANSSI	Recommandée	Résilience	

Remplir le registre des traitements et le tenir à jour	CNIL	Indispensable	Gouvernance	<p>Rapprochez-vous de votre DPD ou de l'équipe juridique pour compléter le registre avec les 6 informations suivantes : les parties prenantes (responsable de traitement, sous-traitants, catégories de destinataires) qui interviennent dans le traitement des données, les catégories de données traitées et de personnes concernées, le but poursuivi (ce que vous faites des données), qui a accès aux données et à qui elles sont communiquées, combien de temps vous les conservez, comment elles sont sécurisées. Plus d'information ici. Le registre est prévu par l'article 30 du RGPD, c'est un outil global avec votre organisme il participe à la documentation de la conformité. Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles.</p> <p>Evaluer le but de chaque collecte de données. Ne collecter que les données strictement nécessaires pour atteindre votre objectif. Il ne faut pas collecter des données inutiles pour votre traitement en se disant qu'elles pourraient servir plus tard. Lorsque trop de données sont collectées, il faut immédiatement supprimer les données non-nécessaires. Cette mesure limite la collecte des données personnelles uniquement aux informations essentielles pour réaliser un objectif spécifique. Cela réduit les risques liés à la gestion des données et renforce la protection de la vie privée des personnes.</p> <p>Ne conserver les données en « base active » (ou environnement de production) que le temps strictement nécessaire à la réalisation de l'objectif poursuivi. Il faut ensuite détruire ou anonymiser les données ou les archiver dans le respect des obligations légales applicables en matière de conservation des archives publiques. Vous pouvez consulter le guide pratique prévu à cet effet. Cette mesure vise à limiter le temps pendant lequel les données personnelles sont conservées et traitées, réduisant ainsi les risques de mauvaise utilisation, d'accès non autorisé, de fuite de données ou de réutilisation non-anticipée.</p>
Minimiser la collecte des données à caractère personnel au strict nécessaire	CNIL	Indispensable	Gouvernance	<p>Ne conserver les données en « base active » (ou environnement de production) que le temps strictement nécessaire à la réalisation de l'objectif poursuivi. Il faut ensuite détruire ou anonymiser les données ou les archiver dans le respect des obligations légales applicables en matière de conservation des archives publiques. Vous pouvez consulter le guide pratique prévu à cet effet. Cette mesure vise à limiter le temps pendant lequel les données personnelles sont conservées et traitées, réduisant ainsi les risques de mauvaise utilisation, d'accès non autorisé, de fuite de données ou de réutilisation non-anticipée.</p>
Déterminer une durée limitée de traitement et de conservation des données à caractère personnel au strict nécessaire	CNIL	Indispensable	Gouvernance	<p>Ne conserver les données en « base active » (ou environnement de production) que le temps strictement nécessaire à la réalisation de l'objectif poursuivi. Il faut ensuite détruire ou anonymiser les données ou les archiver dans le respect des obligations légales applicables en matière de conservation des archives publiques. Vous pouvez consulter le guide pratique prévu à cet effet. Cette mesure vise à limiter le temps pendant lequel les données personnelles sont conservées et traitées, réduisant ainsi les risques de mauvaise utilisation, d'accès non autorisé, de fuite de données ou de réutilisation non-anticipée.</p>

Fournir des informations aux personnes concernées sur l'utilisation de leurs données à caractère personnel	CNIL	Indispensable	Gouvernance	<p>Informers clairement les personnes lors de la collecte de leurs données de manière à ce qu'elles puissent : connaître la raison de la collecte des différentes données les concernant ; comprendre le traitement qui sera fait de leurs données ; être assurées de la maîtrise de leurs données, notamment via l'exercice de leurs droits. La liste complète des informations à fournir est disponible ici. Les personnes doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'elles soient clairement informées de l'utilisation qui sera faite de leurs données. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits. Plus d'information ici.</p> <p>Permettre aux personnes d'exercer leurs droits d'accès aux données qui les concernent, de rectification ou de suppression, voire d'opposition (sauf si le traitement répond à une obligation légale). Une réponse à une demande de droit d'accès doit contenir une copie des données ainsi que : l'objectif du traitement des données, si possible sa durée, l'identité des destinataires, dans le cas d'un traitement automatisé sa logique et ses conséquences. Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée. Plus d'informations sont disponibles ici. Les personnes ont le droit d'accéder aux données à caractère personnel qui ont été collectées à leur sujet. Elles doivent pouvoir exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité.</p> <p>Consulter la liste des exemptions. Si votre traitement n'y figure pas, regarder s'il fait partie des traitements pour lesquels une AIPD est obligatoire. Si une AIPD est nécessaire, vous pouvez la réaliser à l'aide du logiciel PIA. Cette analyse, aussi appelée Analyse d'Impact sur la Protection des Données (AIPD), vise à évaluer et à atténuer les risques liés au traitement des données personnelles, surtout dans le cas de traitements susceptibles de présenter des risques élevés pour les droits et libertés des individus.</p>
Fournir des informations aux personnes concernées sur les modalités d'exercice des droits	CNIL	Indispensable	Gouvernance	
Vérifier si une analyse sur la protection des données à caractère personnel doit être réalisée	CNIL	Indispensable	Gouvernance	

Mettre en œuvre :

- une connexion par SSO conforme au standard SAML V2.0 pour les utilisateurs internes
- une connexion directe par login/mot de passe pour les utilisateurs externes

Mesures
ajoutées

Protection