

Annexe commune

Interopérabilité Microsoft 365, sécurité et coordination avec le prestataire M365 du GIP

Fourniture, préparation et déploiement d'équipements informatiques

Consultation n° 2026-GIPREM-INFO-01

DOCUMENT CONTRACTUEL

Cette annexe s'applique aux deux lots, à proportion des prestations exécutées.

1. Contexte numérique du GIP

Le GIP utilise Microsoft 365. Son environnement comprend notamment Microsoft Entra ID, Microsoft Intune, Windows Autopilot et Microsoft Teams. L'administration, la sécurisation et l'exploitation de cet environnement sont actuellement assurées, pour le compte du GIP, par la société ALOHIA.

Pendant toute la durée du marché, la désignation « prestataire M365 » vise ALOHIA ou tout autre prestataire ultérieurement désigné par le GIP. Le changement de prestataire M365 n'emporte aucune modification de l'objet ou des prix du marché.

2. Principe de coopération

Le titulaire coopère loyalement avec le GIP et le prestataire M365 pour assurer l'interopérabilité, la sécurité, la préparation, le déploiement et le support des équipements. Cette coopération est incluse dans les prix, dans la limite des prestations définies par le marché.

Le prestataire M365 n'est ni un sous-traitant imposé au titulaire ni son cocontractant. Il ne peut facturer directement au titulaire une prestation non prévue. Le titulaire demeure responsable de ses fournitures, de ses interventions et de ses sous-traitants.

3. Répartition des responsabilités

Activité	Titulaire du marché	Prestataire M365	GIP
Fourniture, conformité et garantie des matériels	R	I	A
Transmission des références, numéros de série et empreintes	R	C	A
Paramétrage du tenant, des profils Intune et des politiques	C	R	A
Enregistrement Windows Autopilot	R ou C selon la commande	R ou C	A
Pré-provisionnement et contrôles de conformité	R selon la commande	C / R	A
Installation physique et raccordement	R	C	A
Recette d'interopérabilité	R	C / R	A
Décision d'admission	I	C	R / A
Gestion des comptes et licences	I	R	A

R : responsable de l'exécution ; A : autorité de validation ; C : consulté ou contributeur ; I : informé. Le bon de commande peut préciser la répartition pour une opération déterminée sans transférer la responsabilité contractuelle du titulaire.

4. Obligations de coordination

- désignation d'un interlocuteur technique et d'un suppléant ;
- participation aux réunions ou échanges techniques raisonnablement nécessaires ;
- transmission préalable des informations techniques, numéros de série, fichiers d'import, pilotes et prérequis ;
- signalement immédiat des incompatibilités, dépendances, licences ou actions attendues d'un tiers ;
- planification conjointe des opérations susceptibles d'affecter les agents ou le système d'information ;
- production de comptes rendus ou procès-verbaux lorsque la commande le prévoit.

5. Accès au système d'information

- autorisation préalable du GIP ou du prestataire M365 agissant sur son instruction ;
- compte nominatif, droits minimaux, durée limitée et authentification multifacteur lorsque disponible ;
- interdiction des comptes partagés, sauf impossibilité technique documentée et mesure compensatoire validée ;
- connexion depuis un terminal professionnel maîtrisé, à jour, chiffré et protégé ;
- journalisation des actions administratives et conservation des traces utiles pendant douze mois, lorsque cela est techniquement possible ;
- désactivation immédiate des accès à la fin de l'intervention.

6. Gestion des secrets et informations sensibles

Les mots de passe, jetons, clés, certificats, codes temporaires et informations d'architecture sont échangés par un canal sécurisé distinct des courriels ordinaires lorsque leur sensibilité l'exige. Ils ne figurent pas en clair dans les comptes rendus, tickets ou fichiers de livraison.

Le titulaire ne copie aucune donnée du GIP vers une messagerie personnelle, un support non autorisé ou un service cloud non validé. Les secrets temporaires sont révoqués après usage. Les informations nécessaires à l'exploitation sont restituées au GIP ou déposées dans le mécanisme sécurisé désigné.

7. Exigences de sécurité des équipements

- TPM 2.0 et Secure Boot activés pour les ordinateurs ;
- BIOS/UEFI, micrologiciels et pilotes à jour, signés et issus de sources officielles ;
- absence de mot de passe BIOS inconnu du GIP et remise des éléments nécessaires à l'administration ;
- absence de logiciel de prise en main à distance, compte local ou outil non autorisé ;
- support de BitLocker et conservation des clés dans l'environnement désigné par le GIP ;
- désactivation ou protection des services, ports et interfaces d'administration inutiles.

8. Windows Autopilot et Intune

Lorsqu'elle est commandée, la prestation comprend la production et la transmission d'un fichier compatible avec Windows Autopilot comprenant les champs requis, notamment le numéro de série, l'identifiant de produit et l'empreinte matérielle, ainsi que le group tag communiqué par le GIP lorsqu'il est utilisé.

Le titulaire vérifie que l'équipement n'est pas déjà rattaché à un autre tenant. Toute difficulté d'import ou tout rattachement antérieur est résolu avant l'admission.

Le pré-provisionnement Intune est réalisé exclusivement avec les profils et instructions validés par le GIP ou son prestataire M365. Le titulaire ne modifie aucune politique, aucun groupe, aucun rôle ni aucune configuration du tenant de sa propre initiative.

9. Confidentialité et données personnelles

Sont confidentiels : les informations relatives aux agents, aux comptes, aux équipements, à l'architecture, aux configurations, aux vulnérabilités, aux procédures de sécurité et aux contrats du GIP. Elles ne sont utilisées que pour l'exécution du marché et ne sont communiquées qu'aux personnes ayant à en connaître.

Les données temporaires sont supprimées à la fin de l'intervention. Lorsque le titulaire traite des données personnelles pour le compte du GIP, il agit exclusivement sur instructions documentées, impose la confidentialité à son personnel, met en œuvre les mesures appropriées et assiste le GIP pour la gestion des incidents et des droits des personnes.

10. Incidents de sécurité

Le titulaire signale sans délai, et au plus tard dans les quatre heures ouvrées suivant sa détection, tout incident ou suspicion d'incident susceptible d'affecter le GIP : accès non autorisé, perte d'équipement ou de données, logiciel malveillant, divulgation, erreur de configuration, vulnérabilité critique, fuite de secret ou compromission de la chaîne d'approvisionnement.

- notification initiale précisant la date, le périmètre, les systèmes ou données concernés et les premières mesures prises ;
- point de situation dans les vingt-quatre heures ;
- préservation des journaux et éléments de preuve ;
- plan de remédiation coordonné avec le GIP et le prestataire M365 ;
- rapport final indiquant la cause, la chronologie, les impacts et les mesures de non-récurrence.

11. Vérifications d'interopérabilité

Avant admission, les parties vérifient, selon le périmètre commandé : l'import Autopilot, l'enrôlement Intune, l'application des profils, la conformité et la remontée d'inventaire, les mises à jour, le chiffrement, le fonctionnement de la station d'accueil, du réseau filaire, des deux écrans, de l'audio, de la caméra, de Teams et le bon fonctionnement après redémarrage.

Toute dépendance non annoncée, licence cachée, rattachement à un autre tenant, pilote non supporté ou incompatibilité constitue une non-conformité.

12. Fin d'intervention et réversibilité

- retrait des comptes, droits, certificats et outils temporaires ;
- remise des fichiers, inventaires, procédures et journaux prévus ;
- suppression des copies et données temporaires ;
- transfert des informations nécessaires au GIP ou au prestataire qu'il désigne ;
- attestation de clôture ou d'effacement à la demande du GIP.