

Annexe 1

Équipement des intervenants et travail sur site DGFIP, travail sur site distant, télétravail

1. Équipement des intervenants et travail sur site DGFIP

Chaque représentant du titulaire intervenant pour le compte de la DGFIP sera équipé d'un ordinateur fourni par le titulaire qu'il équipera du socle technique et des outils DGFIP.

Le recours aux logiciels et outils DGFIP pour réaliser les travaux pour le compte de la DGFIP est la norme.

C'est notamment le cas de la suite bureautique (LibreOffice), du client de messagerie, des outils de productivité, des environnements de développement. Lorsque cela est justifié par la nature de l'intervention, des logiciels spécifiques du titulaire peuvent être, après validation, installés sur les postes mis à disposition sous réserve, le cas échéant, que les accords de licence qui pourraient être détenus par le titulaire le permettent.

La connexion d'un ordinateur non équipé du socle DGFIP au réseau de la DGFIP est proscrite.

Si les intervenants sont par ailleurs équipés d'un ordinateur portable fourni et soclé par leur société, celui-ci ne doit pas être connecté au réseau de la DGFIP.

L'utilisation de suites bureautiques tierces est dans le cas général proscrite.

L'utilisation de suites bureautiques, de solution de messagerie ou de conservation de document en nuage, plus largement de solutions autres que celles fournies et hébergées par la DGFIP est proscrite.

Les échanges entre intervenants pour le compte de la DGFIP et avec les agents de la DGFIP se font par l'intermédiaire du compte de messagerie DGFIP mis à disposition.

L'utilisation des moyens mis à disposition de la DGFIP (poste de travail, messagerie, accès internet, etc.) fait l'objet d'une surveillance de conformité d'usage et de sécurité qui peut conduire à des rappels à l'ordre et demande de remise en état, voire, selon la gravité ou en cas de récidive, à demander le retrait d'un intervenant. La charte encadrant l'usage des outils numériques par les représentants du titulaire et le cas échéant, la politique générale de sécurité numérique de la DGFIP, seront tenues à disposition des intervenants, et son acceptation formelle

incluse dans l'accord de discrétion et confidentialité signé par chaque intervenant. De manière générale, les intervenants, comme les agents de la DGFIP, ne disposent pas de droits d'administration sur leur poste. En fonction de l'organisation opérationnelle retenue, il pourra être décidé par la DGFIP de déléguer des droits de soclage ou d'administration des postes de travail des intervenants à des représentants du titulaire bien identifiés chargés de réaliser les opérations privilégiées sur les postes DGFIP utilisés par les représentants du titulaire.

Les travaux d'encadrement de l'exécution du marché et les échanges associés peuvent être réalisés sur les équipements du titulaire (hors réseau DGFIP donc). Les documents échangés devront être aux formats standards DGFIP (OpenDocument compatible avec la suite LibreOffice ou PDF).

Un poste qui serait détecté comme non conforme devra être remis en condition normale d'utilisation du poste au socle DGFIP. Un poste compromis devra être retiré du réseau et éventuellement mis à disposition de la DGFIP pour analyse. Dans les deux cas, le titulaire s'engage à se conformer aux consignes qui lui seront données par la DGFIP.

2. Travail sur site distant

Lorsque l'organisation de la réalisation des prestations objet du présent marché le justifie, certains intervenants peuvent opérer depuis les locaux de la société du titulaire plutôt que dans les locaux de la DGFIP.

Les locaux sur le site du titulaire dans lesquels sont réalisés ces prestations sont alors organisés comme une extension de site DGFIP.

- une empreinte immobilière dédiée, clairement identifiée et sécurisée aux conditions en vigueur pour les sites DGFIP est mise en place sur le site du titulaire ;
- un contrôle d'accès nominatif à cette empreinte est mis en place, dont la traçabilité est tenue à disposition de la DGFIP.

- cette empreinte est reliée au réseau DGFIP en tant que site tiers par l'intermédiaire d'un routeur DGFIP implanté dans l'empreinte dédiée et sécurisée, dans un local technique adapté.

Pour les sites situés hors de France, le fournisseur est tenu d'apporter, dans des conditions identiques à celles mises en œuvre par la DGFIP sur le territoire national et sous son contrôle, l'interconnexion opérateur entre le local dédié et les infrastructures nationales de la DGFIP en Île-de-France.

- ce local technique contient aussi les équipements de commutation dédiés à la distribution du réseau DGFIP auprès de tous les équipements qui doivent être reliés à la DGFIP ; aucun équipement intermédiaire de commutation ou de brassage mutualisé n'est autorisé.

- les postes de travail reliés au réseau DGFIP sont fournis par le titulaire et installés avec le socle et les outils DGFIP, suivant le même principe que des postes utilisés sur un site de la DGFIP

- les règles d'utilisation et de gestion de ces postes, plus largement des moyens mis à disposition, sont les mêmes qu'à l'article 1 ci-dessus.

- les éventuels moyens informatiques mis à disposition par le titulaire, et utilisés depuis les postes connectés au réseau DGFIP sont localisés dans la même empreinte immobilière, ou dans une empreinte répondant aux mêmes conditions et dont l'interconnexion est fournie par la DGFIP.

- pour chaque empreinte connectée à la DGFIP, le titulaire devra établir avec son donneur d'ordre la liste des accès réseau (ouvertures de flux) nécessaires à la réalisation des missions de manière à ce que ces accès soient autorisés sur les dispositifs de filtrage de la DGFIP.

- sauf accord particulier, le travail en jours/heures non ouvrés suivant le calendrier de France métropolitaine depuis un site distant n'est pas autorisé.

En particulier sont interdits :

- toute forme d’interconnexion du réseau et des postes reliés à la DGFIP avec un quelconque réseau tiers.
- toute connexion d’équipements non approuvés par la DGFIP au réseau relié à la DGFIP ; si les intervenants utilisent des postes du titulaire dans l’empreinte réservée à la DGFIP, il est recommandé qu’ils ne disposent que d’une connexion non filaire vers un réseau distribué par le titulaire, de manière à limiter tout risque de connexion de ces postes au réseau filaire relié à la DGFIP.

3. Télétravail

Le télétravail quand il est autorisé, au cas par cas, et en accord avec la DGFIP est réalisé depuis un ordinateur portable en déport d’écran vers le poste de travail habituel socré DGFIP situé dans les locaux de la DGFIP ou sur site distant. Ce poste de travail est obligatoirement un poste fixe fourni par le titulaire (ordinateur portable prohibé).

Le déport d’écran se fait au travers d’un dispositif d’authentification et de traçabilité mis en place par la DGFIP qui mémorise les actions des télétravailleurs.

Sauf accord particulier, le télétravail est réalisé depuis le territoire national, au domicile de l’intervenant ou d’un de ses proches. Le lieu de télétravail est connu de l’employeur qui en tient l’information à disposition de la DGFIP.

Sauf accord particulier, les plages horaires de télétravail sont les jours/heures ouvrés suivant le calendrier de France métropolitaine.

Le télétravail depuis l’étranger est proscrit et soumis à sanction auprès du titulaire du marché. Il entraînera des mesures qui pourront *a minima* bloquer l’utilisation de la connexion à distance voire nécessiter un retour dans une enceinte DGFIP pour sa remise en conformité.

Les conditions d’utilisation des moyens informatiques, notamment le recours exclusif aux outils et moyens accessibles depuis le poste laissé dans les locaux reliés à la DGFIP s’appliquent.

Trois approches distinctes sont envisageables au choix de la DGFIP concernant la modalité d’accès en télétravail :

3.1 l’intervenant utilise un ordinateur portable équipé du socle DGFIP et la collecte VPN DGFIP

C’est le cas général. L’ordinateur portable est fourni par le titulaire et ré-installé avec le socle et les outils de connectivité DGFIP. Les modèles et caractéristiques d’ordinateurs portables peuvent faire l’objet de consignes particulières pour en assurer la compatibilité avec le socle de poste de travail de la DGFIP.

Dans tous les cas le titulaire communique l’ensemble des pilotes nécessaires.

Ce poste est utilisé exclusivement pour se connecter à la DGFIP en VPN aux fins de télétravail.

3.2 l'intervenant utilise un ordinateur portable et la collecte VPN du titulaire

Sous réserve de validation par la DGFIP, le recours à un ordinateur portable fourni et installé par le titulaire, à un dispositif de collecte VPN propre au titulaire, les flux rdp étant routés sur une interconnexion avec la DGFIP vers les postes de travail habituels, est envisageable.

Les points clés qui alimenteront la validation de la DGFIP d'un tel dispositif sont :

- le caractère industriel du déploiement et de l'entretien des postes du titulaire ;
- l'existence de mesures d'application et de contrôle de la conformité des postes et des logiciels installés ;
- les dispositifs de détection et de protection contre les logiciels malveillants mis en place ;
- le recours à un dispositif de filtrage non optionnel du surf et de la messagerie ;
- la nature et le niveau d'entretien de la solution de collecte VPN, ainsi que sa capacité à assurer une connexion permanente, un contrôle de conformité des postes, une ségrégation de la population des intervenants pour le compte de la DGFIP vers un réseau dédié, seul routé vers l'interconnexion à la DGFIP ;
- la capacité du titulaire à garantir l'isolation de bout en bout de cette population, entre la collecte VPN et l'interconnexion avec le réseau DGFIP ;

Le dispositif alors mis en place prend la forme suivante :

- une interconnexion lan2lan IPSEC est mise en place entre un équipement du titulaire et la DGFIP ; ce lan2lan route le flux rdp de déport d'écran depuis les postes de télétravailleurs vers les postes de travail habituels soclés DGFIP ;
- le titulaire définit un profil VPN de poste de travail permettant d'amener les postes de travail des intervenants pour le compte de la DGFIP dans un réseau dédié !
- ce réseau dédié dispose des accès « sortants » vers les services d'infrastructure du titulaire qui permettent l'entretien et la surveillance des postes ;
- ce réseau est le seul routé vers le lan2lan vers la DGFIP.

Le titulaire tient à disposition de la DGFIP les portions pertinentes de journaux d'accès et d'utilisation des infrastructures utilisées dans ce cadre (support au fonctionnement du poste de travail et collecte VPN). La DGFIP se réserve le droit de faire auditer les dispositifs mis en place par le titulaire.

3.3 Télétravail des métiers de l'exploitation

Les situations qui conduisent un intervenant du titulaire à assurer des interventions ponctuelles ou récurrentes sur des environnements de pré-production ou de production se font avec un ordinateur portable DGFIP spécifiquement configuré pour le télétravail des exploitants