

Convention de sécurité



À l'attention des prestataires
intervenant au CID

SOMMAIRE

1.1 OBJET DU DOCUMENT.....	4
1.2 ACTEURS CONCERNÉS.....	4
1.3 RESPONSABILITÉ.....	4
1.4 ALERTE.....	4
2.1 RECOMMANDATIONS GÉNÉRALES	4
2.2 SÉCURITÉ DES POSTES DE TRAVAIL CONNECTÉS SUR LES RÉSEAUX INFORMATIQUES DOUANIERS.....	5
2.3 SÉCURITÉ DES FICHIERS.....	5
2.4 ACCÈS INTERNET.....	6
2.5 CONTRÔLE.....	6
2.6 SYSTÈMES PERSONNELS.....	6
2.7 PHOTOGRAPHIES.....	6
2.8 LA CONVENTION DE DISCRÉTION ET DE CONFIDENTIALITÉ.....	7

1 PRÉSENTATION DU DOCUMENT

1.1 OBJET DU DOCUMENT

Ce document définit les obligations de sécurité et de discrétion imposés par l'Administration aux intervenants des sociétés prestataires lorsqu'ils interviennent au CID.

Le périmètre concerné par cette convention est l'ensemble du système d'information de la douane et en particulier les systèmes techniques hébergés au CID (centre informatique douanier)

1.2 ACTEURS CONCERNÉS

Chaque intervenant devra signer la présente convention de discrétion et de confidentialité.

1.3 RESPONSABILITÉ

Le prestataire et ses intervenants s'engagent via cette convention à ne pas :

- compromettre l'intégrité, la disponibilité et la confidentialité du système d'information de la Douane ;
- diffuser ou favoriser la diffusion d'informations du système d'information de la Douane.

En particulier, les actions du prestataire et de ses intervenants ne doivent pas conduire ou permettre :

- l'installation volontaire ou involontaire de programmes malveillants sur le système d'information de la Douane ;
- le détournement volontaire ou non des logiciels qu'il utilise ;
- la conservation ou la divulgation d'informations confidentielles de la douane et du CID.

1.4 ALERTE

Lorsqu'un événement de sécurité est détecté par un intervenant, celui-ci a l'obligation d'alerter le référent douanier de l'intervention, et le RSSI du CID en cas d'incident de sécurité avéré.

2 CONVENTION DE DISCRÉTION ET DE CONFIDENTIALITÉ

Dans le cadre des dispositions légales et réglementaires en matière de protection de la confidentialité, de l'intégrité et de la disponibilité des données, traitements et documents de la DGDDI, le prestataire et ses intervenants s'engagent à prendre toutes les mesures utiles pour assurer la protection absolue des informations figurant notamment dans les matériels informatiques.

Cette protection s'étend à l'ensemble des supports de quelque nature que ce soit, sans limite de délais et en tous lieux, y compris lorsque ses intervenants se trouvent dans et hors les locaux de l'Administration.

2.1 RECOMMANDATIONS GÉNÉRALES

Chaque intervenant travaillera sur le poste de travail (portable, ...) fourni par sa société. Celui-ci ne sera **jamais connecté sur le réseau de Production du CID**. Si besoin, l'accès au réseau de production de l'intervenant se fera selon les modalités suivantes :

- utilisation d'un poste d'administration de la Douane ;
- accompagnement par un informaticien douanier, référent de l'intervention ;
- les informations d'authentification ne seront pas fournies à l'intervenant.

Il est remis à chaque intervenant lors de son premier jour de mission au CID un exemplaire de la PSIT (politique de sécurité informatique et télécommunications) qu'il est tenu de respecter. La cellule TSI comme le RSSI du CID sont à sa disposition pour lui apporter les éclairages nécessaires.

2.2 SÉCURITÉ DES POSTES DE TRAVAIL CONNECTÉS SUR LES RÉSEAUX INFORMATIQUES DOUANIERS

Le poste de travail de l'intervenant doit respecter les obligations suivantes :

- respect des recommandations de sécurité de l'Anssi applicables ;
- Pas de connexions aux partages réseau douane ;
- Pas de liaison WIFI active ;
- Pas de matériel réseau hors carte Ethernet ;
- Pas de connexions mail directes (hors web-mail) ;
- Configuration du poste selon les instructions de la DGDDI (palier technique) ;
- Aucun outil d'analyse réseau installé ;
- Pas de fonctionnement en mode administrateur (l'utilisation très occasionnelle de ce mode pour les opérations qui le nécessitent est autorisée) ;
- Poste à jour de ses correctifs de sécurité système et applicatifs ;
- Outil antivirus et antispyware à jour (signatures et logiciel) avec des capacités de détection des rootkits ;
- Pas de fonction serveur.

2.3 SÉCURITÉ DES FICHIERS

Les fichiers sont les documents ou logiciels fournis par la DGDDI au titulaire ou remis par le titulaire à la DGDDI. En cas de conservation de ces fichiers de l'Administration sur des supports matériels (poste de travail, Clé USB, DVD...), l'intervenant s'engage à les placer dans un espace encrypté permettant une sécurité suffisante et adaptée à la confidentialité des informations. Il est demandé que cet espace chiffré soit géré par un produit certifié par l'Anssi (par exemple True Crypt).

Attention : en cas de livraison d'un espace encrypté sur un support, le mot de passe est fourni à l'Administration séparément.

Les clés USB ne doivent être utilisées que pour transférer les données et non pas comme un moyen de stockage (risque de perte de données important).

La société prestataire s'engage à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin d'intervention, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

2.4 ACCÈS INTERNET

En aucune façon, l'intervenant ne se connectera à internet via son poste de travail lors de sa présence au CID. Un accès ponctuel à internet sera possible depuis des postes spécialisés en cas de réelle nécessité.

2.5 CONTRÔLE

Le RSSI du CID, ou l'AQSSI, ou tout autre personne mandaté par ceux-ci, pourront procéder à tout moment à un audit de sécurité complet du poste de travail de l'intervenant. L'intervenant est informé que les flux réseau générés à partir de son poste de travail sont journalisés et qu'ils pourront être utilisés à des fins de contrôle.

2.6 SYSTÈMES PERSONNELS

L'intervenant s'engage à ne connecter aucun système personnel (smartphone, baladeur MP3, clé USB personnelle, ...) au système d'information de la Douane.

2.7 PHOTOGRAPHIES

Toute photographie prise à l'occasion de visites dans les bureaux, salles machines ne sera pas exploitée, publiée ou transmise à un tiers sans le consentement écrit préalable du Directeur du Cid.

Ainsi, l'intervenant ne pourra pas utiliser une ou plusieurs de ces photographies confidentielles à quelque fin que ce soit, en dehors de l'exécution de la présente prestation prévue au contrat et notamment ne pas utiliser ces photographies directement ou indirectement, soit dans un but industriel, soit dans un but commercial, soit encore dans un but de recherche.

2.8 LA CONVENTION DE DISCRÉTION ET DE CONFIDENTIALITÉ

Ce document, élaboré par la DGDDI devra être dûment complété et signé par chaque intervenant.

Les supports informatiques et documents fournis par la DGDDI (centre informatique douanier) à la société prestataire..... *[identité du prestataire]* restent la propriété de la DGDDI.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont la société prestataire *[identité du prestataire]* prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, la société prestataire *[identité du prestataire]* s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La société prestataire *[identité du prestataire]* s'engage à respecter les clauses de la présente convention de sécurité pour les prestataires intervenant au CID.

Je soussigné

Prénom :.....
Nom :.....
Qualité :.....

reconnaît avoir pris connaissance des obligations de discrétion du présent document (convention de sécurité des prestations au CID v2.1) et m'engage à respecter l'ensemble de ces obligations. J'autorise le contrôle par l'Administration des matériels dont je dispose et ce, à tout moment.

Fait à Osny, le

Signature de l'intervenant

Visa RSSI CID (Prénom Nom – Date)	Visa Référent DGDDI-CID (Prénom Nom – Date)