DSI DIRECTION DU SYSTÈME D'INFORMATION

# Formulaire individuel - Conditions d'utilisation du VPN (Virtual Private Network ou réseau privé virtuel)

## Objet

Le présent document a pour objet de définir les conditions d'utilisation des accès VPN.

Ces accès sont octroyés par la Direction du Système d'Information (DSI), dans le respect du besoin d'en connaître, exclusivement :

- aux personnels de l'administration, pour accéder à des ressources nécessaires à l'exercice de leurs fonctions ;
- aux intervenants externes dûment autorisés, lorsque le contrat les liant à l'administration le prévoit et pour l'accès aux ressources nécessaires à la réalisation des prestations objets de ce contrat.

Tout autre usage est strictement interdit.

Ces accès sont octroyés, pour une durée déterminée, à des personnes physiques nommément désignées.

## Respect de la charte informatique

La charte informatique (circulaire n° 7726 PR du 1er octobre 2021) s'applique à l'utilisateur qui atteste en avoir pris connaissance et s'engage à la respecter strictement.

Pour consulter la charte service-public.pf/sipf/wp-content/uploads/sites/9/2022/08/CHARTE-INFORMATIQUE-PF.pdf

## Respect de la législation en vigueur

L'utilisateur, quel que soit son pays d'origine, s'engage à respecter la législation en vigueur en Polynésie française. Il veillera avant toute utilisation du VPN à prendre connaissance de cette législation et notamment de la loi Informatique et libertés du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que des dispositions utiles du code pénal qui pourraient s'appliquer en cas de manquement de sa part.

L'utilisateur, personnel de l'administration, est soumis au secret professionnel et aux règles de déontologie fixées par le statut le régissant, notamment l'article 12 du statut de la fonction publique de la Polynésie française.

## Sensibilisation de l'utilisateur

L'utilisateur s'engage à fournir à la DSI, à première demande, une attestation personnelle de sensibilisation ou de formation à la sécurité informatique type MOOC de l'ANSSI https://secnumacademie.gouv.fr/ et/ou à la protection des données personnelles, datant de moins d'un an.

## Sécurité du poste de travail de l'utilisateur

L'utilisateur s'engage à utiliser le VPN sur un poste de travail professionnel conforme aux règles de l'art de la sécurité, telles que préconisées par la DSI. Il met en place les moyens nécessaires, techniques et organisationnels, pour s'assurer que ce poste de travail reste sécurisé dans le temps.

## Sécurité et protection des informations

L'utilisateur s'engage à prendre toutes les mesures utiles afin de préserver la sécurité des informations auxquelles il a accès. Il veille notamment à ce qu'elles ne soient ni déformées, ni endommagées, ni accessibles ou communiquées à des tiers non autorisés, et ce, de façon intentionnelle ou accidentelle.

Il s'engage à détruire toutes les informations mises à sa disposition à la fin de la prestation ou de la convention.

Il s'engage à ne pas compromettre l'intégrité, la disponibilité et la confidentialité du système d'information de la DSI.

L'utilisateur s'engage à suivre les bonnes pratiques dites du « bureau propre et de l'écran vide » (ne pas laisser des informations affichées à l'écran, verrouiller sa session en cas d'absence, choisir un mot de passe de session fort, etc.).

## Accès aux systèmes

L'utilisateur s'interdit d'accéder ou de se maintenir dans un système auquel il n'a pas ou plus vocation à accéder dans ses fonctions ou pour la réalisation de sa mission au bénéfice de l'administration, d'en entraver ou d'en fausser le fonctionnement, d'y introduire frauduleusement des données, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient.

S'il parvient à accéder à des systèmes, données ou autres informations auxquelles il ne devrait pas accéder, ou s'il constate qu'il lui serait possible de le faire, l'utilisateur s'engage à en informer immédiatement la DSI par courriel (support.dsi@administration.gov.pf).

Il s'interdit de conserver tout élément, copie ou support des informations auxquelles il a eu accès et s'engage à les supprimer et à en attester par écrit et sur l'honneur.

Il atteste être parfaitement informé que ces actes peuvent faire l'objet de poursuites sur le fondement des articles 323-1 et suivants du code pénal reproduits ci-après en extraits.

## Analyses et contrôles

Pour assurer un bon fonctionnement et une protection du réseau, la DSI veille au bon usage des ressources des utilisateurs. En conséquence, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau informatique sont analysés et contrôlés, selon les modalités prévues par la charte informatique et dans le respect de la législation applicable, notamment de la loi Informatique et Libertés.

## Responsabilités

L'utilisateur est le seul responsable de son utilisation du service d'accès par VPN.

La DSI peut suspendre l'accès VPN à un utilisateur si ce dernier ne respecte pas les conditions d'utilisation prévues dans le présent document.

## Données personnelles de l'utilisateur

Les données personnelles de l'utilisateur font l'objet d'un traitement géré par la DSI pour le compte du Gouvernement de la Polynésie française, ayant pour finalité la Gestion des accès VPN. Ce traitement est fondé sur son intérêt légitime d'assurer le bon fonctionnement des outils informatiques nécessaires aux missions de l'administration.

Les données sont conservées tant que l'utilisateur est en poste dans l'administration ou en contrat de prestation. Ses données ne sont accessibles qu'aux agents habilités de la DSI.

Il dispose des droits d'accès, de rectification de ses données, de limitation de leur traitement, et dans certaines situations, des droits à l'effacement de ses données et d'opposition à leur traitement. Il peut les exercer à support.dsi@administration.gov.pf ou contacter la déléguée à la protection des données à dpo@administration.gov.pf. Il peut également saisir la CNIL d'une réclamation.

***Extraits du code pénal*** (ces extraits ne présentent pas de caractère exhaustif)

***Atteintes aux systèmes de traitement automatisé de données***

*Article 323-1 : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende ».*

*Article 323-2 : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. »*

*Article 323-3 : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. »*

***Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques***

*Article 226-21 : « Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité …, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.*

*Article 226-22 : « Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.*

*La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence. »*

Par la signature de ce document, l'utilisateur s'engage à utiliser les services VPN conformément aux présentes conditions d'utilisation.

Date de début d'accès* :

Date de fin d'accès* :

Date de l'attestation du MOOC de l'ANSSI* (document à joindre) :

Lister les ressources objets du présent accès* :

Entité/Société :

Référence de la convention/marché :

Nom et Prénom :

Date et lieu :

Signature :