

Document Classe A

Police et procédures FinNet-VPN

1. But

Le but de ce document est de décrire les directives qui sont d'application lors d'une connexion VPN depuis un réseau public et non sécurisé avec FinNet, le réseau privé du SPF Finances.

Le SPF Finances reconnaît la nécessité de fournir à son personnel un accès sécurisé à ses ressources informatiques sur base d'une demande dûment introduite.

Le but recherché n'est pas d'utiliser l'infrastructure VPN pour établir une liaison permanente avec FinNet.

2. Etendue

Le service VPN est une des possibilités offerte par le SPF Finances à ses utilisateurs autorisés d'avoir accès à ses ressources informatiques à partir de sites éloignés.

Cette police concerne chaque utilisateur VPN.

Toutes les autres directives en rapport avec l'utilisation de ressources informatiques (comme le code de déontologie de l'ICT Finances) restent d'application.

3. Police

Ce service VPN est un privilège qui implique un certain nombre de responsabilités tant pour l'utilisateur que pour le SPF Finances.

Les utilisateurs du service FinNet-VPN sont tenus d'avoir, sur leur poste de travail, un programme anti-virus, et de veiller à sa mise-à-jour. Il est également recommandé d'avoir un logiciel pare-feu. Ces logiciels doivent être actifs.

Les utilisateurs sont aussi priés de suivre les "bonnes pratiques" conformément au Code de déontologie ICT afin de sécuriser leur équipement aux accès non autorisés.

Le SPF Finances se réserve le droit de soumettre tous systèmes et communications client VPN à un audit de conformité.

Le service VPN peut être désactivé sans préavis et pour une durée indéterminée pour des raisons de sécurité.

Quand un utilisateur pense que les données relatives à son identification pourraient être connues par un tiers, ou si le matériel servant à son identification a été perdu ou volé, il doit le faire savoir immédiatement au Servicedesk. En outre, il changera le plus vite possible les mots de passe concernés.

La fonction du service VPN de FinNet se limite à fournir un accès sécurisé à l'intranet du SPF Finances. Ce service est orienté « user managed », ce qui signifie que l'utilisateur est lui-même responsable pour le choix d'un F.A.I. (Skynet, Telenet, etc.), l'installation de la connexion à internet et des logiciels associés, y compris les coûts éventuels qui en découlent. En cas de problème lié à l'installation ou à l'utilisation de la connexion VPN, introduisez un « Support Request » auprès du Servicedesk (0257/63636) ou via la page du service.

Du fait de l'utilisation de l'infrastructure VPN, l'utilisateur VPN donne le droit au SPF Finances de réaliser, à tout moment, un audit de conformité sur l'équipement utilisé. Toutes les informations qui sont supposées être traitées par l'infrastructure VPN peuvent être enregistrées dans les buts suivants :

- audit de conformité avec la politique de sécurité
- analyse de problème VPN
- instruction au niveau judiciaire
- enquête interne dans le cadre d'une procédure disciplinaire officielle.

Les infractions commises seront étudiées en profondeur et éventuellement mèneront à des poursuites. L'utilisateur du VPN est tenu de respecter les règles prévues dans le code de déontologie ICT.