Accès au VPN d'Université Côte d'Azur, engagement partenaire ou prestataire

Afin de répondre à l'évolution des cybermenaces, l'Université Côte d'Azur renforce et adapte sa politique de sécurité des systèmes d'information de façon continue. Les accès VPN (Virtual Private Network ou réseaux privés virtuels) constituent, dans ce cadre, un point d'attention particulier.

Le présent engagement s'applique aux partenaires et prestataires se connectant par l'intermédiaire d'un VPN à des ressources mises en œuvre par UCA.

1) Chaque connexion VPN se rapporte à une personne physique nommément identifiée et rattachée à une structure externe donnée (partenaire, prestataire …), l'accès VPN est strictement personnel et ne peut, en aucun cas, être partagé avec un tiers.
2) L'usage de la connexion VPN s'inscrit dans le cadre général de la charte RENATER. Il est exclusivement limité au cadre et aux finalités documentés par UCA et préalablement communiquées au demandeur. La réalisation de toute autre activité est strictement prohibée.
3) Le système d'exploitation du poste ainsi que les logiciels installés doivent être dans une version maintenue par l'éditeur et intégrant les mises à jour de sécurité diffusées à date ;
4) Un dispositif de détection et de suppression des logiciels malveillants éprouvée (antivirus) doit être activé sur le poste, quel que soit son système d'exploitation, dans sa version à jour ;
5) Les espaces de stockages, y compris tout support amovible utilisé, doivent faire l'objet d'une détection complète et régulière ;
6) L'accès au compte utilisateur du poste de travail doit être protégé, à minima, par un mot de passe répondant aux préconisations de l'ANSSI (12 caractères alphanumériques comportant majuscules et minuscules ainsi qu'au moins un caractère spécial) ;
7) Aucune mémorisation des mots de passe d'accès au VPN, aux systèmes et aux services applicatifs opérés par UCA ne doit être réalisée sur le poste de travail ;
8) Toute suspicion d'intrusion ou de compromission du poste doit être immédiatement signalée auprès du référent UCA à l'origine de la demande d'accès ;

Le présent engagement s'applique dans le cadre du partenariat ou de la prestation suivante *(désignation du partenariat / de la prestation, description synthétique des finalités et des ressources correspondantes)* :

Je m'engage par la présente au respect des règles d'usage ci-dessus détaillées. Je suis, enfin, informé que conformément à la loi, les accès aux réseaux et services de l'Université Côte d'Azur sont journalisés pour une durée d'un an. Les données recueillies sont traitées :

- de façon anonyme à des fins d'optimisation et d'exploitation courante ;
- de façon pseudonymisés ou identifiée, en fonction des dispositions légales en vigueur, afin d'assurer la sécurité des équipements et des services opérés par UCA ainsi que la gestion de cyber incidents.

Le demandeur de l'accès VPN	Le responsable légal du partenaire ou du prestataire, à défaut son DSI ou son RSSI	Validation du responsable de la structure d'UCA concerné par le partenariat ou la prestation
Nom, prénom, date et signature	*Nom, prénom, fonctions, date et signature*	*Nom, prénom, fonctions, date et signature*