Clauses de sécurité relatives aux fournisseurs et aux partenaires

Commented [AES1]: Pour apprendre à sélectionner les clauses de sécurité, consultez ces articles :

- 6-step process for handling supplier security according to ISO 27001 https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/
- [illegible]

Lors de l'élaboration d'un accord avec un fournisseur ou un partenaire, les clauses suivantes à inclure dans l'accord doivent être déterminées à partir de la liste suivante (la formulation juridique de l'accord doit être établie par la personne responsable des questions juridiques) :

1. des précisions sur les services fournis, en indiquant les informations qui doivent être accessibles à ces fins et la manière dont les informations sont classifiées, y compris le mappage des schémas lorsque l'organisation et le fournisseur utilisent différents schémas de classification
2. si le fournisseur a le droit d'embaucher des sous-traitants ; si oui, le consentement écrit de l'organisation doit être obtenu, avec une description des mesures que doivent prendre les sous-traitants
3. une définition des informations classifiées et de la manière dont les secrets commerciaux sont réglementés
4. la durée de l'accord et de l'obligation de protéger les informations / secrets commerciaux confidentiels et classifiés après l'expiration de l'accord (lors de la rédaction de cet Article, la manière dont la continuité des activités sera assurée, au sein de l'organisation, doit être prise en compte)
5. le droit de l'organisation d'accéder à des informations conservées ou traitées par le fournisseur / partenaire
6. le droit d'auditer ou de contrôler l'utilisation d'informations confidentielles et de contrôler l'exécution de l'accord dans les installations du fournisseur / partenaire, et de déterminer si les audits peuvent être menés par des tiers ; préciser les droits des auditeurs
7. [illegible]
8. [illegible]
9. [illegible]
10. [illegible]
11. [illegible]
12. [illegible]
13. [illegible]

14. la définition du temps de réponse aux incidents et l'établissement d'un processus d'escalade relatif à la résolution de problèmes et d'incidents
15. les actions résultant de la violation de l'accord ; la responsabilité du fournisseur / partenaire relative aux transactions non réalisées, hors délai ou incorrectes et à d'autres activités sous-traitées
16. la connaissance du fournisseur / partenaire des politiques et procédures clés de l'organisation en matière de sécurité
17. l'obligation de former les employés du fournisseur / partenaire à toutes les activités dans lesquelles ils sont impliqués
18. veiller à ce que les fournisseurs / partenaires soient conscients de la nécessité de sécurité
19. l'interdiction aux employés de l'organisation de transférer aux fournisseurs / partenaires tout actif informationnel, sans en être dûment autorisé par le propriétaire de l'actif
20. l'objectif de niveau de service et le niveau de service inacceptable
21. la définition de critères de performance de service, y compris l'efficacité des mesures, de leur contrôle et de leur présentation
22. une définition précise du système et du format de rapport
23. un processus de gestion du changement précisément défini
24. le système de contrôle d'accès – définir les raisons d'accorder des droits d'accès aux tiers, les processus de connexions et de mots de passe autorisés, les processus d'autorisation pour l'accès des utilisateurs individuels et l'octroi des privilèges, l'obligation de conserver un enregistrement de tous les utilisateurs et de leurs droits d'accès, le processus de suppression des droits d'accès

[illegible]