

Clauses de sécurité relatives aux fournisseurs et aux partenaires

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

1. les parties s'engagent, après l'expiration de l'accord commercial, à assurer la sécurité et l'intégrité des informations confidentielles, y compris l'établissement de protocoles pour assurer la protection des informations confidentielles et pour assurer la continuité des activités au sein de l'organisation
2. l'identification et l'utilisation de mesures de sécurité pour assurer la protection des actifs de l'organisation, y compris les contrôles d'accès, les mesures pour la protection contre les vols, les incendies, les mesures de protection physique, y compris pour la protection de l'intégrité, de la confidentialité et de la disponibilité des informations, y compris pour assurer la confidentialité de la destruction des actifs informationnels après leur utilisation, y compris pour assurer la copie et la diffusion des informations, y compris pour assurer la sécurité de l'organisation, de développement et de maintenance des systèmes d'information et des systèmes de sécurité informationnels
3. après l'accord sur les aspects financiers, les aspects d'adhésion internes et externes, et les autres aspects relatifs aux opérations commerciales des fournisseurs / partenaires, qui gouvernent les partenariats avec l'organisation
4. les responsabilités et les actions des parties à l'accord des personnes physiques des personnes non autorisées aux informations par les contrôleurs personnes après l'accord de ce engagement peuvent dépasser des droits d'accès aux informations, etc.)
5. l'identification de propriétaires de l'information et de la manière dont les droits de propriété confidentielle sont réglementés
6. l'identification des informations classifiées et d'accès accordés, l'accès à ces informations pour les besoins de ces informations et de ces accès
7. le processus permettant d'identifier l'accès aux informations, les mesures et les responsabilités de sécurité, ainsi que l'accès aux données aux informations, les contrôles de la confidentialité, ou tout autre accord ou engagement contractuel

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/>

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
25. une clause relative à l'obligation de tous les droits d'accès qui ne sont pas explicitement autorisés
26. le droit de contrôler et de surveiller toute activité relative aux actifs de l'organisation
27. les mesures pour assurer la confidentialité des activités, en conformité avec les politiques de l'organisation - identifier les services qui nécessitent des niveaux et le délai requis
28. la responsabilité quant aux dommages en cas de rupture des relations contractuelles, y compris la responsabilité relative en cas de violation de la confidentialité de l'information en cas de non-réalisation de services
29. la responsabilité de l'organisation / partenaire relative à la conservation des données en conformité avec les réglementations
30. les conditions relatives à la prolongation ou à la violation de l'accord
31. le langage de l'accord et de la future communication entre l'organisation et les fournisseurs / partenaires
32. les exigences concernant les exigences légales, réglementaires et contractuelles applicables à l'organisation et à son fournisseur, y compris tout niveau des exigences qui doit respecter l'organisation
33. l'objectif de niveau de sécurité et le niveau de sécurité acceptable
34. les exigences de formation et de sensibilisation relatives à certaines activités sensibles
35. les contrats, telles que concernant les questions de sécurité de l'information et d'intégrité
36. les exigences concernant l'indivisibilité possible, lorsque la loi l'autorise, de personnel de l'organisation
37. le processus de résolution des conflits
38. les modifications apportées aux contrats de travail des employés de l'organisation, pour inclure les clauses de sécurité de l'information qui le doivent respecter
39. les fonctions et responsabilités en matière de sécurité de l'information relatives à l'organisation et au fournisseur
40. les mesures prises par l'organisation et celles prises par le fournisseur de services cloud