Security Clauses for Suppliers and Partners

the person responsible for legal matters):

1. details about the service provided, specifying information to be made available for this
2.
   subcontractors
3. a definition of classified information and how trade secrets are regulated
4.
5.
   supplier/partner
6. the right to audit or monitor the use of confidential information and to monitor agreement
7.
8.
   ensure the return or destruction of information assets after their use, controls to prevent copying and distributing information, controls for secure acquisition, development and maintenance of information systems and information security systems
9.
10.
11.
12.
13.
14. defining the incident response time, and establishing an escalation process for problem and incident resolution
15. actions ensuing from breach of agreement; responsibility of the supplier/partner for unperformed, untimely or incorrect transactions and other contracted activities
16.
17.
    involved
18. ensuring that suppliers/partners are aware of the need for security

Commented [270011]: To learn how to select the security clauses, read these 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/
- Which security clauses to use for supplier agreements? https://advisera.com/27001academy/blog/2017/06/19/which-security-clauses-to-use-for-supplier-agreements/

19. [illegible] assets without proper authorization of the asset owner
20. [illegible]
21. [illegible]
22. [illegible]
23. a precisely specified change management process
24. access control system – define reasons for third-party access rights, permitted log-in and [illegible]
25. [illegible]
26. [illegible]
27. controls to ensure business continuity, in accordance with the organization's priorities – which services need to recover within which deadline
28. responsibility for damage in case of breach of contractual relations, including material liability in case of breach of confidentiality of information or in case of non-performance of services
29. [illegible]
30. [illegible]
31. [illegible]
32. [illegible]
33. target security level and unacceptable security level
34. [illegible]
35. [illegible]
36. [illegible]
37. [illegible]
38. [illegible]
39. [illegible]
40. controls managed by the organization and those managed by the cloud service provider