Security Clauses for Clients, Suppliers and Partners

1. Security Clauses for Cloud Services' Clients

1.1. Clauses for general cloud service provision

When drawing up an agreement as a Cloud Service Provider, it must be defined which of the [illegible]

1. [illegible]
2. [illegible] subcontractors
3. the definition of the organization's point of contact (person or department to act as the focal [illegible]
4. [illegible] under the contract
5. the allocation of information security roles and responsibilities between the organization (as the Cloud Service Provider), its suppliers involved in the cloud service provisioning, and the [illegible]
6. [illegible] Cloud Service Provider)
7. the identification of the geographical locations of the organization (as the Cloud Service [illegible]
8. information about legal requirements the organization (as the Cloud Service Provider), and [illegible]
9. [illegible]
   - any intended changes that can impact the cloud service operations or data security
   - [illegible]
   - [illegible]
10. information, in a way that does not disclose information that can be improperly used, about:
    - [illegible]
    - [illegible]
    - [illegible] service customer
    - arrangements for the disposal and reuse of resources
    - [illegible]

Commented [27A1]: 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/

Commented [27A2]: Depending upon the cloud model adopted, [illegible]

Commented [27A3]: E.g.: Law enforcement authorities, regulatory bodies, etc.

Commented [27A4]: E.g., law enforcement agencies to be [illegible]

Commented [27A5]: E.g.: practices for international transfer of [illegible]

Commented [27A6]: E.g.: changes in geographical locations [illegible]

Commented [27A7]: E.g.: [illegible]

Commented [27A8]: E.g.: upon the termination of the cloud service use agreement or change of cloud service sub-contractor.

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

- [redacted]
- [redacted]
- time reference used by the cloud systems, and how the cloud service customer can synchronize local clocks with the cloud service time reference
- [redacted]

11. information about cloud service functionalities, in a way that do not disclose information that can be improperly used, that are available to the cloud service customer and allow it to:
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - report information security incidents
12. [redacted]
    - monitor the use of cloud services and resource capacity
    - [redacted]
13. use of non-disclosure agreements with those who may have access to detailed information [redacted]

[redacted]

agreement, the cloud service customer should be consulted.

Commented [27A9]: Depending upon the available [redacted]

Commented [27A10]: The cloud service customer's information [redacted]

1.2. Clauses for cloud service provision as a PII processor

[redacted]

clauses will be included in the agreement (the legal wording of the agreement must be prepared by the person responsible for legal matters):

Commented [27A11]: Contracts and agreements are legal [redacted]

1. [redacted]
2. [redacted] the Cloud PII Processor), its sub-contractors, and the cloud service customer, concerning the fulfillment of PII protection
3. [redacted]
4. the definition of the organization's point of contact (person or department to act as focal [redacted]
5. [redacted]
6. information, in a way that does not disclose information that can be improperly used, about:

Commented [27A12]: E.g.: credit card data, healthcare data, financial data, etc.

Commented [27A13]: E.g.: IaaS, PaaS or SaaS

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

- [redacted]
- [redacted]
- [redacted]
- [redacted] restoration efforts
- arrangements for the disposal and reuse of resources that may store PII data
- [redacted]
- controls applied to protect data logs gathered and stored related to the processing and use of the cloud service customer's PII
- [redacted]

7. [redacted]
   - manage its users access
   - manage its PII data
   - [redacted]
   - [redacted]
   - [redacted]
8. the assurance to:
   - [redacted]
   - [redacted]
   - [redacted] bound or authorized by the cloud service customer (consider the use of non-disclosure agreements)
   - [redacted]
   - [redacted]
9. the identification of the geographical locations of the organization (as cloud PII provider) and [redacted]

Note: It should be observed that the cloud service customer may have its own clauses to be included [redacted]

Commented [27A14]: [redacted]

Commented [27A15]: The cloud service customer's information [redacted]

2. Security Clauses for Suppliers and Partners

[redacted] the person responsible for legal matters.):

1. [redacted]

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

2. [illegible]
3. a definition of classified information and how trade secrets are regulated
4. the duration of the agreement and of the obligation to keep confidential and classified [illegible]
5. [illegible] supplier/partner
6. the right to audit or monitor the use of confidential information and to monitor agreement [illegible]
7. [illegible] and to ensure business continuity in the organization
8. identification and use of key controls to ensure the protection of organizational assets – e.g. [illegible] and distributing information
9. [illegible]
10. [illegible] agreement by unauthorized people (e.g. only persons with the need to know may have access rights to information, etc.)
11. [illegible]
12. [illegible]
13. [illegible]
14. defining the incident response time, and establishing an escalation process for problem and incident resolution
15. [illegible]
16. [illegible]
17. [illegible] involved
18. ensuring that suppliers/partners are aware of the need for security
19. [illegible]
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. the right to monitor and revoke any activity related to the organization's assets

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

27. [illegible]
28. [illegible] services
29. responsibility of the supplier/partner to store data in accordance with regulations
30. [illegible]
31. [illegible]
32. [illegible] cloud service customers (e.g.: number of processor cores for application, storage capacity available, network bandwidth available), during particular periods and usage peaks
33. [illegible]
34. availability of evidence that the supplier's or partners' supply chain can maintain or exceed the information security levels defined by [organization name] and by its cloud service customers
35. [illegible]

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.