SECURITY QUESTIONS NEXTEER ASKS CLOUD SAAS PROVIDERS

Access Control

1. Do you help customers support existing credentials and password policies?

2. Do you offer or support SAML/SSO capabilities for authentication?

3. What types of multifactor authentication are supported?

4. How is customer data or processes protected from unauthorized access?

5. What measures do you have in place to prevent unauthorized viewing of information?

6. Who at your premises can see customer data?

7. What measures do you have in place to prevent unauthorized copying, or emailing of customer data?

8. Do you use a multi-tenant server model?

9. What measures do you have to isolate individual tenant systems and data?

10. What additional controls for administrators/high privilege roles exist?

Data Protection

11. What if any data processing limitations exist for your platform or service?

12. What obligations do you fulfill related to the use and disclosure of information?

13. What obligations do you commit to regarding information retention and destruction?

14. What actions do you do to destroy data after it is released by a customer?

15. What happens in the event of data corruption?

16. Do you take responsibility for security and integrity of customer systems and data?

17. Do you encrypt data in transit and at rest?

18. What will happen to our applications and data if you go out of business?

19. How can you ensure customer data won’t become the property of creditors?

Disaster Recovery

20. What are your disaster recovery processes?

21. What are your methods for backing up our data? What are offerings to back up data?

22. How does the cloud service sustain operations during disasters affecting data centers or connections, and which data is backed up where?

23. What is your backup and disaster recovery strategy?

24. How often are incremental backups made?

25. How many copies of data do you store and where are they stored?

26. How far back do the backup copies go?

27. How often and how do you test your backup and recovery infrastructure?

Incident Response

28. Do you have an incident response plan?

29. Do you include customers in the incident response process?

30. Do you provide reports of attempted or successful breaches of systems, impacts, and actions taken?

31. What type of security incidents are mitigated by you?

32. Which tasks and incidents remain under the responsibility of the customer?

33. How can the customer monitor the service, which logs are kept, and how can they be accessed, for example, when the customer needs to analyze an incident?

34. What type of security tasks are carried out by you?

35. What visibility is offered customers into security processes and events affecting data?

Legal Processes

36. What is your process for responding to a legal hold request?

37. How is security of the cloud service guaranteed when there are legal issues or administrative disputes? How do you ensure that personnel work securely under such conditions?

38. How do you ensure legal action taken against other tenants will not affect access to our data?

Organizational Controls

39. What security certifications do you currently hold for your data centers?

40. How often do you have external security assessments performed?

41. Can you provide your third-party security assessment documents (SOC1, SOC2)?

42. Can customers visit a data center and do our own inspection?

Physical Security

43. How does you screen your employees and contractors? Do those screening procedures differ at different international locations? How?

44. Where is your data center, and what physical security measures are in place?

45. What countries is data stored in - both on your infrastructure and for backups?

46. What physical security measures, processes, and monitoring capabilities does you have in place to prevent unauthorized access to its data centers and infrastructure?

Regulatory Compliance

47. Do you comply or plan to comply with privacy regulations (e.g. Privacy Shield, GDPR)?

48. Will you sign a Data Processing Agreement (DPA) to assure us you have the appropriate administrative, physical and technical safeguards to protect all data particularly personal data

49. If your company stores data in non-U.S. locations can the we, the customer specify where we want our data stored? How can we ensure our data will not be stored in other locations?

Service Level Agreements (SLA)

50. How scalable is your solution, including disaster recovery?

51. How reliable is your network infrastructure?

52. What is your current uptime and SLA commitment? What if SLA is not met?

53. Do you alert customers of important changes (e.g. security practices, data center locations)?

54. What must a customer know in in case he/she decide to change SaaS providers?

55. Do you offer periodic reports confirming compliance with security requirements and SLA's?

56. What is the remediation process if the provider cannot live up to your security obligations?

57. If we decide to switch providers or take our systems and data in house, what will it take and what assistance will be given to us to migrate our systems and data?

Software Security

58. How do you ensure software security?

59. How do you determine which software remains customer's responsibility?

60. How is access to the GUI's and API's protected?