Visory

Vendor Assessment Worksheet

QUESTION	ANSWERS / COMMENTS
Data Centers	
Are the data centers in the US?	
Are the data centers operated and maintained by your company or a third-party entity?	
Are the data centers certified or audited to ensure compliance with industry standards such as ISO 27001 or SOC 2?	
Is Data encrypted in transit and at rest?	
Employee Access to Client Data:	
Are there documented access controls and procedures to monitor and track employee access to client data?	
Is data privacy and security training provided to your employees?	
Data Ownership and Confidentiality:	
Who owns the data stored in your application? (e.g. client, vendor)	
Does your agreement contain provisions ensuring the confidentiality and non-disclosure of client data?	
How long is data retained after a client offboards?	
What is the uptime guarantee or SLA in the event of a disaster to your networks or infrastructure?	
Have your disaster recovery and business continuity plans been tested?	
If asked, can you provide documentation or evidence of independent security audits or certifications conducted on your application or infrastructure?	
How do you ensure compliance with relevant data protection regulations, such as SOC 2 Type 2, GDPR or HIPAA?	
Are there any sub-processors or subcontractors involved in the processing of client data?	
How frequently do you perform vulnerability assessments and penetration testing on your application and infrastructure?	
Can you describe your incident response plan and the steps taken in the event of a security breach?	
How do you manage software updates and security patches for your application to ensure protection against known vulnerabilities?	
Have there been any past service interruptions or downtime incidents? If so, how long did they last and how were clients notified?	