Security Questionnaire

Simple Vendor Assessment v1.0, Ericius Security Company, CC-BY-SA-4.

When engaging with a vendor that will store, receive, or process your sensitive information, purchasing software as a service (SaaS), or selecting a cloud service to integrate with your operations, you should briefly stop to consider how risky that service is—and how security will help manage or defend the new tool. Below is a brief security questionnaire you can use to start or guide the security discussion with potential vendors:

1 Vendor Info

1.1 Cost and Value

Question	Answer
Vendor Name	
Cost	
Term of Agreement	
Billing period	
Cancellation Notice Due	
What does your service do?	
What value do you provide? Why should we purchase your services?	

1.2 Regulations

Question	Answer
What compliance standards are you required to meet? (for example, GDPR, HIPAA, SOX…)	
What security certifications do you maintain (for example, ISO, HITRUST, ITIL, SOC 2 Type II, etc)	

2 Security and Risk Controls

2.1 Access Management

Question	Answer
Do you support Single Sign-on (SSO/SAML)?	
Do you support multi-factor authentication (MFA)?	
Can we see or control which of our users haven't applied MFA or who sign-in without SSO?	
What passwords standards can we set for our users?	
How do you manage identities across domains? What API integrations do you support?	

How do you manage your developers', engineers', or administrators' access to our accounts?	
How do you prevent unauthorized access to our accounts or account take over attacks?	
What conditional access controls do you provide?	
How do you help us manage roles? How can we control the scope of each role?	
What access controls or auditing do you have in place for your administrators or engineers?	
Do you require MFA for remote access for all your employees, regardless of privilege level?	
How do you separate users, tenants, and/or administrator access levels?	

2.2 DATA

Question	Answer
Who owns our data when it is stored on your systems? Us or you?	
How and where is our data stored?	
Do we have any say in where our data is stored? (e.g. Country or Region)	
How is our data protected? Do you implement full disk encryption? Download restrictions?	
How is our data kept separate from other customers' data?	
How long is our data retained for while we do business with you? Afterwards?	
Do YOU have access to our data? What do YOU use our data for?	

2.3 IT OPERATIONS

Question	Answer
Do you keep an inventory of your assets according to how important they are?	
How often are your systems patched? (e.g., how often are critical and high security patches managed)	
Do you rely on any systems or software that are past end-of-life?	
How do you backup your systems?	
How large is your: **- Cybersecurity Staff** **- IT Staff** **- Development Team** **- Engineering Team** **- Security Operations Center**	
How does management support cybersecurity efforts and personnel?	

2.4 SECURITY OPERATIONS

Question	Answer
Have you ever been breached? What happened? How did you identify it?	
What happens if you are breached? Do you have an incident response plan?	
If you are breached, how and when will you communicate it to us?	
What level of cybersecurity insurance coverage do you carry?	
How do you monitor the health, availability, and security of your services?	
How do you monitor for threats and cybersecurity incidents?	
Do you have a 24x7 On-call Incident Response Team?	
Are you able to aid us in the event of an incident or investigation?	
What have you done to protect your company from ransomware (or to recover from it)?	
When did you last conduct a vulnerability assessment, risk assessment, or penetration test with an external assessor?	

3 REFERENCES

1. Yu, Sounil. *Cyber Defense Matrix*. Morrisville: JupiterOne, 2022
2. “Resources.” Github. Ericius Security, 2023. https://github.com/ericiussecurity/Resources
3. “7 SaaS security risks that every business should address.” Vendr.com. Vendr, 2022. https://www.vendr.com/blog/saas-security