VENDOR RISK REVIEW GUIDE

A simple red, yellow, green framework for reviewing technology vendors

Step One

CLASSIFY THE VENDOR

If a vendor fits more than one level, use the higher-risk level.

GREEN — LOW RISK

- Public information only
- No personal data
- No confidential business information
- No connection to internal systems

Examples: public website content, general marketing materials, public product information.

YELLOW — MODERATE RISK

- Business contact information
- Limited customer or lead data
- Limited internal information
- Limited system access

Examples: names, work email addresses, phone numbers, job titles or basic lead information.

RED — HIGH RISK

- Sensitive personal or financial data
- Broad or admin system access
- Confidential business information

Examples: payroll, payment data, CRM access, employee records or AI processing sensitive business data.

When in doubt, move up a level

A vendor that mostly handles business contact information may still be RED if it has broad CRM access, administrator rights, or another connection that could expose sensitive data. The rating should reflect the most serious thing the vendor can see, change, store or expose.

Step Two

MATCH THE REVIEW TO THE RISK

Once the vendor is classified, use these questions to dig into how they will keep your data secured.

Questions to answer	GREEN	YELLOW	RED
What data will the vendor collect, store or access?	•	•	•
Does the privacy policy explain what it collects, how it uses it, and how we can manage or delete it?	•	•	•
Does the vendor need all of the data and access it is requesting?	•	•	•
Is there an appropriate services agreement or contract in place?	•	•	•
Is our data encrypted while it is being transmitted?	–	•	•
Is our data encrypted while it is stored?	–	•	•
Does the vendor use MFA and appropriate access controls?	–	•	•
What is the vendor allowed to use our data for?	–	•	•
Can our data be used to train or improve AI models?	If AI	•	•
How long will the vendor keep our data?	–	•	•
What happens to our data when we stop using the service?	–	•	•
Who are the vendor's subprocessors, and will we be told when they change?	–	•	•
How and when will the vendor notify us about a security breach?	–	•	•
Do the contract and, when needed, DPA document these protections?	–	•	•
Can the vendor provide security documentation or a trust center?	–	As Needed	•
For high-risk vendors, is SOC 2, ISO 27001 or similar evidence available?	–	–	•
For high-risk vendors, did we complete a formal security risk assessment?	–	–	•
Will we review and reclassify this vendor at least annually?	–	•	•

• = required As needed = use judgment based on the data, access and contract If AI = only when the vendor uses AI

Red flags that should move a vendor up a level

- The vendor cannot clearly explain what data it collects or why.
- It asks for broader system access than seems necessary.
- It cannot provide basic security documentation or explain how it protects data.
- It will not explain AI use, subprocessors, retention or deletion.
- Its contract allows broad reuse of your data.