QUICK REFERENCE

Vendor Risk Assessment Checklist

A practical due-diligence framework for evaluating the vendors who touch your data or network.

Why This Matters

Your vendors often have access to your systems, data, or network. If a criminal compromises them, they can pivot straight into your business. Target was breached in 2013 through their HVAC vendor — 40 million card numbers stolen. Your security is only as strong as the weakest vendor you grant access to.

Questions to Ask Before You Sign

For any vendor with access to your data or systems

✓ **What security training do your employees receive?** *Good answer: regular training with specific policies. Bad: "We have not really thought about that."*

✓ **Do you carry cyber insurance?** *Should be at least $1 million. Ask for a certificate of insurance.*

✓ **Where will you store our data?** *Good: specific data-center locations, ideally in-country. Bad: "Wherever is cheapest."*

✓ **What happens to our data when we end the relationship?** *Good: deleted within 30 days with written confirmation. Bad: kept indefinitely.*

✓ **Have you had any security incidents in the past 3 years?** *Be wary if they say "no" — everyone has had something. Be encouraged if they describe what happened and what they fixed.*

For IT vendors and software companies

✓ **What security certifications do you hold?** *Look for SOC 2 or ISO 27001. Absence is not automatic disqualification, but ask how they prove their practices instead.*

For anyone handling sensitive customer data

✓ **How do you encrypt our data?** *Should encrypt both at rest (stored) and in transit (being sent). If they cannot explain this clearly, they probably are not doing it.*

Essential Contract Clauses

Work with your lawyer to include these:

- **Data ownership:** "All data belongs to [Your Company]. Vendor may not use it for any other purpose."
- **Breach notification:** "Vendor will notify us within 24 hours of any security incident involving our data."
- **Right to audit:** "We may request evidence of your security practices at any time."
- **Insurance floor:** "Vendor maintains cyber liability insurance of at least $1,000,000."
- **Data deletion:** "Within 30 days of contract end, vendor will delete all our data and provide written confirmation."
- **Liability:** "Vendor is liable for damages resulting from their security failures."

Managing Vendor Access — Least Privilege

✓ Create a separate login for each vendor — never share yours

✓ Grant only the access they actually need to do the job

✓ Set an expiration date on every vendor account

✓ Remove access immediately when the work ends

✓ Review all vendor access every 3 months (quarterly audit)

Red Flags to Walk Away From

- They refuse to answer security questions ("that is proprietary")
- They cannot or will not provide proof of insurance
- They want to use your personal account instead of a vendor account
- They ask for more access than the work reasonably requires
- They cannot clearly explain their security measures
- They have had multiple incidents with no evidence of fixes
- They are dramatically cheaper than competitors — shortcuts in security are a common reason why

Simple Vendor Tracking Sheet

Keep a spreadsheet with:

- Vendor name and what they do for you
- What data or systems they access
- Primary contact and contact information
- Contract expiration date
- Last security review date
- Cyber insurance on file? (Y / N)
- Notes and any red flags observed

Review the sheet quarterly. Update it whenever you onboard or offboard a vendor.

If a Vendor Gets Breached

Find out what data was involved and when. Assess your risk — was it your customer data? Change passwords for any systems they access. Review your systems for suspicious activity. Consider temporarily suspending their access. Contact your lawyer and cyber insurance. Document every communication.