# Third-Party Risk Checklist for Small Businesses

Editable Vendor Vetting, Tracking & Review Template

## 📋 SECTION 1: Vendor Vetting – Before You Sign

* Initial Due Diligence

☐ Identify service provided and data accessed

☐ Request and review security certifications (SOC 2, ISO 27001, etc.)

☐ Review vendor’s privacy policy and data handling practices

☐ Assess breach notification process and incident response plan

☐ Perform risk classification: ☐ Low ☐ Medium ☐ High

* Contractual Safeguards

☐ Sign a Data Processing Agreement (if handling personal data)

☐ Include confidentiality and security obligations in contract

☐ Specify data deletion or return obligations

☐ Include audit rights or compliance evidence requirements

## 🗂️ SECTION 2: Vendor Tracking – Maintain Oversight

* Vendor Registry

☐ Record vendor name, service, and access level

☐ Document contract start and end dates

☐ Assign internal owner or point of contact

* Ongoing Oversight

☐ Monitor vendor performance and SLA compliance

☐ Conduct annual risk/compliance check-ins

☐ Track breach or incident notifications

☐ Subscribe to vendor security update feeds

## 🔁 SECTION 3: Annual Review & Offboarding

* Annual Review

☐ Reassess risk and access levels

☐ Confirm continuing need for the vendor

☐ Evaluate cost vs. value vs. risk

* Offboarding Checklist

☐ Revoke access to systems and data

☐ Secure return or certified deletion of company data

☐ Retrieve any devices or assets

☐ Document all offboarding steps

## 🧰 Suggested Tools for Management

|  |  |
| --- | --- |
| Task | Tools |
| Vendor Tracking | Excel, Notion, Vendorful, Torii |
| Compliance Assessment | Whistic, Vanta, Drata |
| Policy/Contract Templates | Termly, OneTrust, TrustArc |