# Vendor Security Checklist

# (for Small & Mid-Sized Businesses)

*How to use:*

* *Run a quick huddle (≤15 minutes).*
* *For each item, circle Yes / Partly / No and assign an Owner and Due date.*

*Scoring: Yes = 2, Partly = 1, No = 0. Sum your score and use the action plan.*

horizontal line

# Section A — Must-Pass Gates (Failure = Reject Vendor):

1. Vendor identity verified through independent sources?  
   ☐ Yes ☐ No
2. No sanctions, fraud, or conflict-of-interest flags?

☐ Yes ☐ No

1. Signed code of conduct and compliance agreement?  
   ☐ Yes ☐ No
2. Meets critical security and data protection requirements?  
   ☐ Yes ☐ No

## Section B — Verification & Controls

1. Vendor registration documents validated?

☐ Yes ☐ Partly ☐ No

1. Background checks and references completed?  
    ☐ Yes ☐ Partly ☐ No
2. Ownership and beneficial owner disclosed?

☐ Yes ☐ Partly ☐ No ☐

## Section C — Data & Privacy

1. Data handling and retention policy reviewed?  
   ☐ Yes ☐ Partly ☐ No
2. GDPR/CCPA compliance confirmed if applicable?

☐ Yes ☐ Partly ☐ No

1. AI/data use practices disclosed and approved?

☐ Yes ☐ Partly ☐ No

## Section D — Security & Access

1. Information security certifications in place (ISO 27001, SOC2)?  
   ☐ Yes ☐ Partly ☐ No
2. Access controls and monitoring enforced?  
    ☐ Yes ☐ Partly ☐ No
3. Incident response and breach notification process clear?  
    ☐ Yes ☐ Partly ☐ No

## Section E — Oversight & Responsible Use

1. Signed contract includes compliance clauses?  
   ☐ Yes ☐ Partly ☐ No
2. Vendor performance reviewed at least annually?  
    ☐ Yes ☐ Partly ☐ No
3. Exit/termination plan defined and tested?  
    ☐ Yes ☐ Partly ☐ No

## Scoring Evaluation:

* **32–40 (Low risk):** Keep momentum. Move to the **Pro Toolkit** to formalize templates.
* **20–31 (Moderate):** Fix quick wins in 14 days. Schedule a 2-hour workshop.
* **0–19 (High):** Freeze new AI tools; enable approvals; run a 30-day sprint to close gaps

## Scoring Evaluation:

* ISO/IEC 42001 (AI Management)
* NIST AI RMF.
* ISO/IEC 27001 (Security)
* EU AI Act.
* GDPR.

*Disclaimer: Operational best practice, not legal advice.*