NexSecure Solutions

Cybersecurity for small businesses, founders, and growing teams

How to use this checklist

This checklist is built to help small teams catch obvious AI risk before it becomes a customer, security, compliance, or trust problem. Use it as a fast review tool. It is not legal advice, and it is not a complete compliance program.

Best for

Small business owners, solopreneurs, SaaS founders, consultants, vibe coders, and teams using tools such as ChatGPT, Microsoft Copilot, Gemini, Grammarly, Jasper, Cursor, Replit, Claude Code, GitHub Copilot, and other AI-enabled platforms.

Step	Action
1	Download or print the checklist.
2	

AI Tool Inventory

Checklist item	Done	In progress	Not started
List all AI tools in use across your business, including ChatGPT, Microsoft Copilot, Gemini, Grammarly, Jasper, and others.	[ ]	[ ]	[ ]
Identify AI features embedded in SaaS tools you already use, such as CRM, HR, accounting, email, design, help desk, and project tools.	[ ]	[ ]	[ ]
Confirm who has access to each AI tool and what permissions they have.	[ ]	[ ]	[ ]
Identify any shared accounts or unmanaged personal accounts being used for business work.	[ ]	[ ]	[ ]

Data Exposure

Checklist item	Done	In progress	Not started

AI-Assisted Development

Checklist item	Done	In progress	Not started
Identify which AI coding tools are being used, including GitHub Copilot, Cursor, Replit, Claude Code, ChatGPT, and similar tools.	[ ]	[ ]	[ ]
Review AI-generated code before it reaches production, especially authentication, authorization, and admin access logic.	[ ]	[ ]	[ ]
Confirm API keys, tokens, secrets, and credentials are not exposed in prompts, code, repositories, logs, screenshots, or AI tool history.	[ ]	[ ]	[ ]
Review whether AI agents or automations can access files, databases, customer records, source code, cloud accounts, or business systems.	[ ]	[ ]	[ ]
Document what human review is required before AI-generated features go live.	[ ]	[ ]	[ ]

Before You Ship

Checklist item	Done	In progress	Not started
Confirm the product does not expose customer data through AI features.	[ ]	[ ]	[ ]
Confirm AI outputs are reviewed or constrained when they affect users, payments, accounts, support decisions, or business decisions.	[ ]	[ ]	[ ]
Confirm logging does not capture sensitive prompts, credentials, customer records, tokens, or private business data.	[ ]	[ ]	[ ]
Confirm AI vendors and APIs have been reviewed for data retention, privacy terms, and security responsibilities.	[ ]	[ ]	[ ]
Confirm you can explain your AI use clearly to a customer, investor, insurer, auditor, or enterprise buyer.	[ ]	[ ]	[ ]

Oversight and Accountability

Checklist item	Done	In progress	Not started
Assign ownership of AI governance decisions, even if it is just you for now.	[ ]	[ ]	[ ]
Create a simple process for reviewing new AI tools before adoption.	[ ]	[ ]	[ ]
Schedule a quarterly review of your AI tool inventory.	[ ]	[ ]	[ ]
Define who can approve AI use in customer-facing workflows or production systems.	[ ]	[ ]	[ ]

Documentation			
Checklist item	**Done**	**In progress**	**Not started**
Document your AI tools, usage policies, and risk controls in writing.	[ ]	[ ]	[ ]
Keep vendor terms, security docs, privacy statements, and data processing agreements on file.	[ ]	[ ]	[ ]
If you are pursuing SOC 2 readiness, cyber insurance, or larger customers, confirm what they expect around AI tool use.	[ ]	[ ]	[ ]
Keep a simple record of decisions, approvals, exceptions, and review dates.	[ ]	[ ]	[ ]

Quick Score

Count how many items you marked Not Started. Use the score below to choose your next step.

Not Started items	What it means	Recommended action
0-5	Basic AI governance is forming.	Focus on documentation, review cycles, and keeping your AI inventory current.
6-12	Moderate unmanaged AI risk.	Start with tool inventory, data exposure, acceptable use, and vendor review.
13+	High unmanaged AI risk.	Do not scale AI use or ship AI-assisted workflows until ownership, data handling, and review controls are clear.

Framework alignment

This checklist is informed by practical AI governance concepts from the NIST AI Risk Management Framework, ISO/IEC 42001, and OWASP guidance for large language model applications. These references help connect everyday AI use to

Next Step

Turn this checklist into a working AI governance plan.

If you marked three or more items Not Started, begin with AI tool inventory, data exposure, acceptable use, and vendor review. If you build software, also review AI-assisted development and Before You Ship before new features go live.

For founders and builders

Speed is useful. Unreviewed AI workflows can still create security debt. NexSecure helps small teams ship without exposing customer data, secrets, production systems, or trust.

Schedule Free Assessment

Use this if you want help deciding where to start.

AI Governance Service

Use this if you want to learn about the service.