# 60-MINUTE SECURITY AUDIT™

## 01: The Basics

**Company Name:**

**Date:**

### 1 Do you hold a current SOC 2 Type II or ISO 27001:2022 certification? If so, is there a dashboard we can use to follow real-time compliance throughout the year?

*These certifications prove an independent auditor has verified the vendor's security controls over time, not just in a one-off check. Best-in-class companies provide a real-time trust center that provides access to a real-time attestation of conformance to controls.*

- SOC 2 Type II: ☐ Yes ☐ No
- ISO 27001:2022: ☐ Yes ☐ No
- Dashboard link:
- Comments:

RED FLAG

*"We follow SOC 2 principles" (but have no report) or relying solely on their cloud provider's (e.g., AWS) security. The ISO 27001 standard was refreshed in 2022. In 2026, there are risks if a company is still adhering to the older 2013 standard.*

### 2 Do you carry dedicated Cyber Liability Insurance?

*General business liability insurance often excludes cyber incidents. If a vendor causes a breach, you need to know they have a specific policy to cover forensic investigations and lawsuits rather than going bankrupt and leaving you with the bill.*

- ☐ Yes ☐ No
- Carrier:
- Coverage amount:
- Comments:

RED FLAG

*"Our general liability policy covers it" or coverage limits under $1M.*

© 2026 Worthwhile Adventures LLC.

# 01: The Basics

## 3 Is customer PII (Personally Identifiable Information) and video data encrypted at rest and in transit?

*Without this, data is readable by anyone intercepting the connection, leaving it vulnerable to immediate theft or future 'harvest now, decrypt later' quantum attacks.*

- In transit: ☐ Yes ☐ No
- At rest: ☐ Yes ☐ No
- What algorithms are used in transit?
- What algorithms are used at rest?
- Comments:

RED FLAG

*They can't name specific algorithms (e.g., AES-256, TLS 1.3) or lack a post-quantum cryptography roadmap*

## 4 Is your platform protected by a firewall?

*Without a properly configured firewall, your platform is essentially sitting on the open street with the front door wide open to automated "bot" attacks and hackers.*

- ☐ Yes ☐ No
- How often is the configuration tested?
- What was the date of the last test?
- Comments:

RED FLAG

*No regular testing schedule for firewall configurations*

## 5 Do you enforce Multi-Factor Authentication (MFA)?

*Passwords are easily stolen or bought on the dark web. If a vendor's support staff can access your data without MFA, your data is one "phishing" email away from being exposed.*

- Do you enforce MFA for all internal staff with access to customer data?
  ☐ Yes ☐ No
- Does your platform require supporting MFA? ☐ Yes ☐ No
- Comments:

RED FLAG

*"We encourage it but don't enforce it" or "Only for admins."*

© 2026 Worthwhile Adventures LLC.

# 01: The Basics

## 6 Can you provide your most recent penetration test summary report?

*Penetration testing is like a fire drill for your digital security. It involves hiring ethical hackers to intentionally try to break into the system to find weaknesses before real criminals do. A report from 2023 or older is useless in 2026.*

- ☐ Yes ☐ No
- Conducted by:
- Conducted date:
- Number of critical issues found:
- Number of high issues found:
- Number of medium issues found:
- Number of low issues found:
- Were all issues resolved? ☐ Yes ☐ No
- What date was the last issue fixed?
- Comments:

RED FLAG

*The vendor has no report, refuses to share a summary report, or the report is more than 12 months old. Another red flag is if the report shows "Critical" or "High" vulnerabilities that remain unresolved months after the test.*

## 7 Do you maintain a formal process such as a Vulnerability Disclosure or Bug Bounty Program for external vulnerability reporting?

*Even the best internal security teams can miss vulnerabilities. Ethical hackers often discover these blind spots in the wild. Without a dedicated reporting channel, critical warnings get lost in general support queues or well-meaning researchers face legal threats. A Vulnerability Disclosure or Bug Bounty Program ensures these external findings are safely reported and patched before attackers can exploit them.*

- ☐ Yes ☐ No
- Link to policy:
- Comments:

RED FLAG

*Directing reports to a general support email, claiming internal testing catches everything, or lacking a safe harbor policy to protect well-intentioned researchers.*

© 2026 Worthwhile Adventures LLC.

# 02: AI & Data Rights

## 8 Is sensitive personally identifiable information (names, credit cards) redacted before being processed by AI?

*Once sensitive data enters an AI model, it can be nearly impossible to "un-bake the cake". Redaction protects you from legal liability under GDPR or CCPA*

- ☐ Yes ☐ No ☐ Not applicable
- Comments:

RED FLAG

*"We trust the AI provider's privacy policy" or no mention of data minimization or automated redaction.*

## 9 Do you use public cloud AI models (like ChatGPT, Gemini, or Claude) or do you develop your own models?

*Public models often use your data to train future versions. A "walled-garden" ensures your customer's data never leaves a secure vault that you control.*

- Public cloud models: ☐ Yes ☐ No
- In-house models: ☐ Yes ☐ No
- Comments:

RED FLAG

*Using standard consumer AI accounts instead of enterprise-grade, isolated environments.*

## 10 Who owns the output of the AI?

*You don't want the vendor claiming they own your customer lists or the resulting estimates after you've spent years feeding them data. You need a contract stating the "work product" belongs to you.*

Answer:

RED FLAG

*Terms that grant the vendor ownership or broad "usage rights" to your generated data.*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

# 02: AI & Data Rights

## 11 Do you comply with the EU AI Act's transparency requirements?

*The EU AI Act is the world's strictest AI law with fines up to 7% of global turnover. If your software uses AI to interact with customers (like a chatbot) or analyze their private data (like a video survey), you are legally required to tell them.*

- ☐ Yes ☐ No
- Comments:

RED FLAG

*No visible labels or notifications telling customers that AI is being used.*

## 12 Does your app store customer videos/photos locally on the device?

*If a surveyor leaves their iPad at a coffee shop, you don't want a stranger accessing your customer's entire home video inventory. Secure apps upload data to the cloud immediately and wipe it from the device.*

- ☐ Yes ☐ No
- Comments:

RED FLAG

*Photos/videos remain in the device's "Camera Roll" or "Gallery."*

## 13 Where is your data physically hosted?

*Privacy laws like GDPR strictly regulate cross-border transfers, and some government contracts require "US Eyes Only".*

- Data processing location:
- Primary data storage location:
- Backup data storage location:
- Comments:

RED FLAG

*Hosting data in jurisdictions with weak privacy laws where it could be seized without consent.*

© 2026 Worthwhile Adventures LLC.

# 02: AI & Data Rights

## 14 What controls do you have in place for GDPR and CCPA?

*Even if you aren't in Europe, principles like the "Right to be Forgotten" are now standard in US laws (CCPA). You need a vendor that offers a hard delete button, or you can risk fines and legal liability.*

- Answer:

RED FLAG *No process to delete customer data*

## 15 Do you have a dedicated Data Protection Officer (DPO) or Security Lead?

*Security cannot be a "side hustle" for the CEO or a general developer. If no one person is accountable for data protection, then effectively no one is. In the event of a breach or audit, you need a specific point of contact who understands the regulatory landscape and the company's security architecture.*

- ☐ Yes ☐ No
- Name:
- Email:
- Phone number:
- Job title:
- Comments:

RED FLAG *A non-technical contact or individual without significant authority at the organization.*

## 16 Please provide your subprocessor list of vendors who process customer data.

*You aren't just hiring a software company; you are indirectly hiring every vendor they use. If they hide their vendor list, you have no way of knowing if your customer data is being sent to a cheap, insecure server overseas or a disreputable organization.*

- For each company, please include the legal name and the purpose the company serves in your tech stack.
- Comments:

RED FLAG *Refusal to share the list or claiming "We don't use vendors."*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

## 17 Do you vet your subprocessors?

*You're only as strong as the weakest link in the chain. If your software provider uses a cheap, unvetted firm for their database management, your data is at risk regardless of how secure the main app is. You need to know that their vendors are held to the same high standards as you hold them.*

- ☐ Yes ☐ No
- If so, what are your requirements?
- Comments:

RED FLAG

*Hosting data in jurisdictions with weak privacy laws where it could be seized without consent.*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

# 03: The "Bad Day" Test

## 18 What is your backup policy?

*Ransomware attackers now actively hunt for backups to overwrite or delete them, destroying your ability to recover. Immutable backups prevent this by strictly denying any command to modify or remove data, guaranteeing a clean restore point remains available.*

- Answer:
- Are your backups immutable? ☐ Yes ☐ No
- How are backups protected?
- Comments:

RED FLAG

*"We back up daily" (without mentioning data residency or immutability).*

## 19 What is your Recovery Point Objective (RPO) and Recovery Time Objective (RTO)?

*These metrics are the physical boundaries of your business's survival. RPO determines how much data you can afford to lose (measured in time since the last backup), while RTO determines how long your business can stay offline before the damage becomes irreversible. For a mover, a bad RPO means losing a whole day of video surveys; a bad RTO means your sales team can't book moves for 48 hours during peak season.*

- RPO:
- RTO:
- Comments:

RED FLAG

*RPO over 1 hour, RTO over 4 hours*

## 20 What uptime percentage was your platform designed for?

*Availability is a design objective among professional engineering firms, not a best-effort basis. You need a vendor that treats availability as a core engineering requirement.*

- Answer:
- Comments:

RED FLAG

*Anything lower than 99.9% uptime.*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

# 03: The "Bad Day" Test

## 21 Do you have a publicly available status page for tracking your platform's uptime?

*Real-time transparency is proof of maturity. A public page proves they aren't "hiding the bodies" when things go wrong.*

- ☐ Yes ☐ No
- If yes, please provide the link:
- Comments:

RED FLAG *"Just email support if it's down."*

## 22 Do you have an Incident Response Plan?

*When a problem happens, you don't want a team that is panicking and winging it. You need a tested playbook to recover quickly.*

- ☐ Yes ☐ No
- How often do you test the plan?
- When was the date of the last test?
- Comments:

RED FLAG *No formal plan or recent test*

## 23 What protections do you have in place to ensure email integrity?

*If a hacker spoofs your email, they can trick customers into wiring money to a criminal. You need cryptographic proof that blocks fake emails before they reach the inbox.*

- For emails sent from your employees:
- For emails sent from your platform:
- Comments:

RED FLAG *Missing DMARC or SPF records on their domain*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

# 03: The "Bad Day" Test

**24** **Do you monitor the dark web for leaked credentials to your platform?**

*Most hacks in 2026 are not technical, they are the result of human failures. You need proactive scanning to close the door before a criminal walks in.*

- ☐ Yes ☐ No
- If yes, how often?
- Comments:

RED FLAG

*No threat intelligence or dark web monitoring.*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

# 04: The Human Element

## 25 What software environments do you have?

*Software should never be built or tested on the same system that holds active customer moves. Mistakes in testing can delete real data or trigger fake emails to actual clients.*

- Answer:
- How do you safeguard data isolation across environments?

- Comments:

RED FLAG

*No isolation between development and production environments or live customer data in non-production environments*

## 26 Do you have a human-in-the-loop review process for AI accuracy?

*AI is prone to "hallucinations", or confidently stating facts that are wrong. A "Human-in-the-Loop" ensures that a qualified expert reviews and validates AI outputs before they reach your customer. This oversight is a key requirement for emerging standards (like ISO 42001) and builds trust with skeptical clients.*

- ☐ Yes ☐ No
- Comments:

RED FLAG

*"Our AI is 100% accurate" or relying fully on automated systems without an ability to audit the results.*

## 27 Do you perform background checks on all employees and contractors with access to production data?

*You wouldn't let a mover into a customer's home without a background check; you shouldn't let a software engineer into their digital home without one either.*

- ☐ Yes ☐ No
- Comments:

RED FLAG

*"We trust our hiring process" (No formal background check policy) or "Only for US employees."*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**

# 04: The Human Element

## 28 Are your employees and contractors required to sign confidentiality (NDA) agreements?

*An NDA ensures that if an employee leaves or goes rogue, they are legally barred from taking your customer lists or trade secrets with them.*

- ☐ Yes ☐ No
- Comments:

RED FLAG

*No formal NDA signed by the first day of work.*

## 29 Do you revoke access for employees and contractors within 24 hours of termination?

*A disgruntled former employee can be your biggest security threat. If their access isn't cut when they leave, they can steal customer lists, export private data, or sabotage systems before anyone realizes they still have access.*

- ☐ Yes ☐ No
- Comments:

RED FLAG

*Manual offboarding processes that take days or weeks.*

## 30 Are all employees trained on security practices?

*Your data is only as secure as the person who just clicked a link in a phishing email. Security training turns your staff from a liability into a "human firewall." Without regular training on social engineering and password hygiene, one mistake by a tired employee can bypass millions of dollars in technical security.*

- ☐ Yes ☐ No
- If yes, how often?
- Comments:

RED FLAG

*Manual offboarding processes that take days or weeks.*

© 2026 Worthwhile Adventures LLC.
Get your 60-Minute Security Audit™ at **zachrattner.com**