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?**

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

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

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

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

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

4 **Is your platform protected by a firewall?**

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

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

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

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

- ☐ 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:

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

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

02: AI & Data Rights

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

- ☐ Yes ☐ No ☐ Not applicable
- Comments:

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

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

10 **Who owns the output of the AI?**

- Answer:

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

- ☐ Yes ☐ No
- Comments:

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

- ☐ Yes ☐ No
- Comments:

13 **Where is your data physically hosted?**

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

02: AI & Data Rights

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

- Answer:

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

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

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

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

17 **Do you vet your subprocessors?**

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

03: The "Bad Day" Test

18 **What is your backup policy?**

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

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

- RPO:
- RTO:
- Comments:

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

- Answer:
- Comments:

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

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

22 **Do you have an Incident Response Plan?**

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

03: The "Bad Day" Test

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

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

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

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

25 **What software environments do you have?**

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

- Comments:

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

- ☐ Yes ☐ No
- Comments:

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

- ☐ Yes ☐ No
- Comments:

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

- ☐ Yes ☐ No
- Comments:

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

- ☐ Yes ☐ No
- Comments:

30 **Are all employees trained on security practices?**

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