Startup Security Questionnaire Response Guide

A Packet33 resource for SaaS and HealthTech founders

If an enterprise prospect, investor, or auditor has sent you a security questionnaire, this guide walks through the categories they typically ask about and how to frame your answers, even if some of these programs are still maturing at your stage.

How to Use This Guide

Enterprise security questionnaires vary in length and format, but almost all of them cluster around the same core categories. You do not need a perfect answer in every category to pass a review. You need clear, honest answers that show you understand your own environment and have a plan for the gaps.

1. Data Handling and Encryption

What they are asking: How is customer data classified, stored, and protected, both at rest and in transit.

What to include:

- Encryption standards in use (e.g. TLS 1.2+ in transit, AES-256 at rest)
- Where data is physically/logically stored (cloud provider, region)
- Data classification approach, even if informal at your stage
- Data retention and deletion practices

> **Framing tip:** If you use a major cloud provider's managed encryption (AWS KMS, GCP's default encryption, etc.), say so explicitly. Reviewers recognize these as strong defaults.

2. Access Control

What they are asking: Who can access customer data, and how is that access limited and monitored.

What to include:

- Role-based access control (RBAC) approach
- Multi-factor authentication (MFA) enforcement, internally and for customer-facing accounts
- Principle of least privilege for engineering/admin access
- Offboarding process when an employee leaves

Framing tip: Even a lightweight, documented process is a legitimate answer. Reviewers are checking for intentionality, not enterprise-scale IAM tooling.

3. Incident Response

What they are asking: What happens if you have a security incident, and how would they find out.
What to include:

- Whether you have a written incident response plan (even a simple one)
- Notification timelines and commitments (many enterprise contracts expect 24-72 hour notification)
- Who owns incident response internally

Framing tip: If you do not yet have a formal plan, this is worth building before you need it; a one-page plan is far better than none, and reviewers can tell the difference between "we have never thought about this" and "we have a plan, it is lightweight."

4. Vulnerability Management and Penetration Testing

What they are asking: Do you test your own security, and how often.

What to include:

- Whether you have completed a third-party penetration test, and how recently
- Whether testing is manual, automated, or both
- Your patching/remediation cadence for identified issues

Framing tip: This is the single most common gap that stalls an enterprise deal for early-stage companies. If you do not have a recent pentest, this is usually the fastest way to unblock a deal. Reviewers frequently ask for the report itself or a summary of findings and remediation.

5. Compliance Certifications

What they are asking: Do you hold or are you pursuing SOC 2, ISO 27001, HIPAA compliance, or similar.

What to include:

- Current certification status (in progress, Type I, Type II, etc.)
- Target completion date if in progress
- Relevant frameworks for your industry (HIPAA for HealthTech, PCI DSS if handling payments)

Framing tip: "In progress, targeting completion by [date]" is a completely normal and acceptable answer for an early-stage company. Reviewers expect a roadmap, not a finished certification, from a Series A company.

6. Subprocessor and Vendor Management

What they are asking: Which third parties touch your customers' data (cloud providers, analytics tools,

support platforms, etc.).

What to include:

- A list of key subprocessors (cloud host, payment processor, email/support tools)
- Whether you review subprocessor security postures before adoption

> **Framing tip:** A simple, maintained list is sufficient at this stage. This is also a good internal exercise to run once, even outside of a questionnaire.

7. Business Continuity

What they are asking: What happens if your infrastructure goes down, and how would you recover.

What to include:

- Backup frequency and location
- Uptime/availability commitments if you have them
- Basic disaster recovery approach

> **Framing tip:** Cloud-native startups often inherit strong defaults here from their infrastructure provider. State what you inherit versus what you have built yourself.

Bonus Points

Using a Compliance Platform like Vanta, Drata, Secureframe, etc.

It makes proving your controls and policies exist in practice, and not only in writing much easier. It also allows you to have a public trust page and automate responses to security questionnaires.

A Note on Honesty

Security questionnaires are not a test you either pass or fail outright. Reviewers on the other end have seen hundreds of early-stage companies and generally understand that a Series A startup will not have enterprise-grade maturity in every category. What erodes trust is vague or evasive answers, not an honest "not yet, here is our plan." Clear gaps with a credible roadmap consistently perform better than answers that overstate your current state.