SaaS Vendor Security Assessment Questionnaire

1. Vendor Information

Company Name

Website

Contact Name

Contact Email

Contact Phone

2. General Information

Describe your SaaS product and its primary business function.

Data hosted/stored (types of data, e.g., PII, PHI, Financial, etc.).

Data storage location(s) (country, region, cloud provider, etc.).

3. Security Policies & Standards

Do you have formal information security policies and procedures?

Are your policies reviewed and updated regularly?

Specify any external security certifications (e.g., ISO 27001, SOC 2).

4. Access Control

Describe user authentication and authorization controls (e.g., MFA, RBAC).

How is access managed for employees and customers?

5. Data Protection

Are data in transit and at rest encrypted?

Describe your data backup and retention strategy.

How is data disposal handled?

6. Application Security

Are regular security assessments or penetration tests performed?

Describe your vulnerability management process.

Do you follow secure software development practices?

7. Incident Response

Do you have a formal incident response plan?

Have you experienced any security incidents in the past 24 months?

If Yes, provide details.

8. Vendor Management

Do you assess the security of your own vendors or sub-processors?

List your main sub-processors.

9. Additional Comments