

Vendor Security Due Diligence Questionnaire

General Information

Vendor Name

Contact Name

Contact Email

Contact Phone

Service(s) Provided

Information Security Policies

Do you have an information security policy?

If yes, how often is it reviewed and updated?

Are employees required to acknowledge the security policy?

Data Protection

What types of data do you process on behalf of clients?

Is sensitive or personal data encrypted at rest?

Is data encrypted in transit?

Access Control

Do you use multi-factor authentication?

How is user access to systems managed and reviewed?

How are accounts removed when no longer required?

Incident Management

Do you have a documented incident response plan?

How are clients notified of data breaches or incidents?

Compliance

Have you completed any third-party security audits or certifications?

If yes, please specify (e.g., ISO 27001, SOC 2):

Are you compliant with applicable data protection regulations (e.g., GDPR, CCPA)?

Additional Comments