SOLTEN VENTURES PUBLIC POLICY

Confidentiality & Information Handling

Public principles for handling non-public business information shared in connection with inquiries, evaluations, and client engagements.

Effective date	September 1, 2026
Applies to	All Covered Properties that link to or adopt this policy

Solten Ventures and its brands may receive non-public business information before and during professional engagements. This policy describes the general information-handling principles we intend to apply across the Covered Properties. It is a public policy, not a substitute for a non-disclosure agreement ("NDA") or the confidentiality provisions of a client engagement agreement.

1. Scope

Solten Ventures and the brands, websites, products, and services that link to or expressly adopt this policy, including Woldmark, DueCap, Solten & Co., and other properties operated by Solten Ventures (collectively, the "Covered Properties").

This policy applies to non-public information shared with us in connection with a business inquiry, fit discussion, due-diligence process, research request, review, analysis, or other professional engagement, subject to any more specific written agreement between the parties.

2. What we treat as confidential business information

Confidential business information may include non-public information about a company's:

- financial performance, forecasts, cash position, budgets, pricing, and unit economics;
- customers, contracts, retention, pipeline, sales performance, and commercial terms;
- products, roadmaps, technology, intellectual property, data, and operating processes;
- employees, contractors, compensation, organization, hiring, and management matters;
- strategy, transactions, financing, investors, board matters, risks, and internal decisions;
- management reporting, analyses, presentations, documents, datasets, and correspondence; and
- other information that is marked confidential or that a reasonable person would understand to be non-public and commercially sensitive in context.

3. Core handling principles

Our general approach is to:

- use confidential business information only for the purpose for which it was provided or as otherwise agreed;
- request only information reasonably relevant to the inquiry or engagement;
- limit access to people and service providers who reasonably need the information for the applicable purpose;
- avoid public disclosure of identifiable client or prospective-client confidential information without permission;
- use reasonable administrative, technical, and organizational safeguards appropriate to the sensitivity of the information; and
- identify material information gaps, uncertainties, or inconsistencies rather than silently treating incomplete information as verified fact.

4. Prospective-client information

For an initial inquiry or fit conversation, we encourage prospective clients to provide only the information reasonably needed to explain the company, the management context, and the reason for seeking an outside review. Highly sensitive documents generally do not need to be submitted through a public website form.

If an NDA is appropriate before detailed information is shared, the parties may put one in place before the substantive review begins.

5. Client information and working materials

During an engagement, we may create notes, analyses, calculations, working papers, summaries, or draft materials derived from client-provided information. The treatment, ownership, delivery, and retention of engagement materials may be further defined in the applicable engagement agreement.

Our role in an independent review is analytical. Unless expressly agreed otherwise, we do not audit, certify, or independently verify all information provided by a client. Conclusions may therefore depend on the completeness and accuracy of the information supplied.

6. Third-party service providers and technology

We may use third-party technology and professional service providers to support hosting, communications, scheduling, file storage, document processing, analytics, security, payment processing, research, and other business operations. Where a provider may process confidential business information, we seek to use the provider only as reasonably necessary for the applicable purpose and subject to appropriate confidentiality, security, or contractual protections where practicable.

The specific providers and technologies used may change over time. A client may raise material security, data-location, or technology-use requirements before an engagement begins so that they can be addressed in the engagement terms where appropriate.

7. Use of information for research, publications, and case examples

We do not intend to publish identifiable confidential client information, client names, internal metrics, documents, quotations, or case details without permission.

We may develop general know-how, analytical methods, and non-client-specific insights through our work. We may use aggregated or de-identified observations for research or internal learning only where the resulting material does not reasonably identify a client or reveal its confidential information, and subject to any stricter contractual commitments in an engagement agreement.

8. Information that is not confidential

Unless a separate agreement provides otherwise, confidential treatment generally does not apply to information that:

- is or becomes publicly available through no breach of an obligation owed by us;
- was lawfully known to us without a confidentiality obligation before disclosure;
- is received lawfully from a third party without a confidentiality restriction;
- is independently developed without use of the confidential information; or
- the information owner authorizes us in writing to disclose.

9. Required disclosure

We may disclose information where required by applicable law, regulation, court order, subpoena, or other valid legal process. Where legally permitted and reasonably practicable, we may notify the affected party before disclosure so that it can seek appropriate protection.

10. Retention and deletion

We may retain confidential business information and related working materials for the period reasonably necessary to perform the relevant purpose, maintain business and legal records, support continuity of an ongoing engagement, resolve disputes, protect legal rights, and satisfy applicable legal, tax, accounting, security, or compliance obligations.

Specific deletion, return, or retention requirements may be agreed in an NDA or engagement agreement. Backup systems and legally required records may not always be capable of immediate deletion.

11. Security incidents

If we become aware of a material security incident involving confidential business information, we will assess the incident and take reasonable steps appropriate to the circumstances. Where notification is required by law or contract, we will provide notice in accordance with the applicable requirement.

12. Relationship to NDAs and engagement agreements

This policy states general public principles only. It does not create a standalone NDA or expand contractual obligations beyond those imposed by applicable law or an agreement between the parties. If an NDA, engagement agreement, data-processing agreement, or other written contract contains different or more specific confidentiality terms, that agreement controls for the covered relationship.

13. Changes to this policy

We may update this policy as our services, technologies, and operating practices evolve. The effective date at the top identifies the current public version. Changes do not reduce contractual confidentiality obligations already agreed in a separate written agreement.

Contact

Questions about this policy may be submitted through the contact details published on the applicable Covered Property. If your inquiry relates to a specific Solten Ventures brand or service, please identify that brand or service in your message.