



Mutual Nondisclosure Agreement

Fillable business-to-business template for preliminary project and technology discussions

Important: This template is not legal advice and is not effective until completed and signed by authorized representatives of both parties. Have counsel review it for the parties, jurisdiction, project, data, employment relationships, and regulatory requirements.

1. PARTIES, PURPOSE, AND KEY TERMS

Effective date *

Agreement term

Party A legal name (Vai-Nova entity) *

Entity type and jurisdiction *

Party B legal name *

Entity type and jurisdiction *

Confidentiality period after disclosure

Project or discussion reference

Purpose of discussions and permitted use *

2. AGREEMENT FRAMEWORK

Each party may disclose Confidential Information and may receive Confidential Information. A party disclosing information is a **Disclosing Party**; a party receiving it is a **Receiving Party**. The obligations below apply equally to both parties.

Do not place passwords, private keys, access tokens, production credentials, regulated records, or export-controlled information into this public template or send them by ordinary email. Secure exchange methods and project-specific controls should be agreed separately.



3. Confidential Information

"Confidential Information" means nonpublic information disclosed by or for a Disclosing Party in any form that is marked or identified as confidential, or that a reasonable person would understand to be confidential from its nature or the circumstances. It may include business plans, pricing, customer and vendor information, technical data, designs, source code, models, prompts, software, architecture, security information, configurations, credentials shared through an approved secure method, system diagrams, research, prototypes, inventions, trade secrets, personal information, and the nonpublic substance of the parties' discussions. Oral or visual information should be identified as confidential when disclosed and summarized in writing within 30 days, unless its confidential nature is otherwise clear.

4. Exclusions

Confidential Information does not include information that the Receiving Party can document: (a) is or becomes public through no breach of this Agreement; (b) was lawfully known without a duty of confidentiality before disclosure; (c) is received lawfully from a third party without a duty of confidentiality; (d) is independently developed without use of the Disclosing Party's Confidential Information; or (e) is released for disclosure in writing by the Disclosing Party.

5. Use and Protection

The Receiving Party will: (a) use Confidential Information only for the Purpose; (b) protect it with at least reasonable care and no less than the care used for its own information of similar sensitivity; (c) limit access to Representatives who have a need to know for the Purpose; (d) not disclose it except as permitted by this Agreement; and (e) not copy, reproduce, or retain it beyond what is reasonably necessary for the Purpose.

6. Representatives

"Representatives" means a party's employees, officers, directors, professional advisers, contractors, and service providers who need the information for the Purpose and are bound by confidentiality duties at least as protective as this Agreement or by professional duties of confidentiality. The Receiving Party is responsible for a Representative's breach to the extent permitted by law.

7. No Reverse Engineering

Unless the Disclosing Party gives prior written permission, the Receiving Party will not reverse engineer, decompile, disassemble, derive source code from, or analyze the composition of nonpublic software, models, samples, prototypes, hardware, or other tangible materials supplied under this Agreement, except to the extent a restriction is prohibited by applicable law.



8. Security and AI Handling

The Receiving Party will apply reasonable administrative, technical, and physical safeguards appropriate to the information and approved environment. Without the Disclosing Party's prior written authorization, the Receiving Party will not: (a) submit Confidential Information to a public or consumer generative AI service; (b) permit a third-party AI provider to train a model on it; (c) use it for public benchmarking, demonstrations, or marketing; or (d) move it into an unapproved hosting, cloud, or colocation environment. Approved private, dedicated, or contractually protected AI systems may be used only within the written scope and controls agreed by the parties.

9. Security Incidents

The Receiving Party will promptly notify the Disclosing Party after discovering unauthorized access, use, loss, or disclosure of Confidential Information. The Receiving Party will take reasonable steps to contain and mitigate the incident, preserve relevant evidence, cooperate in a reasonable investigation, and provide information needed for legally required notices. Notice does not by itself constitute an admission of fault.

10. Required Disclosure

A Receiving Party may disclose Confidential Information when required by law, regulation, subpoena, court order, or valid governmental demand. To the extent legally permitted, it will give prompt written notice, reasonably cooperate with efforts to seek confidential treatment or a protective order, and disclose only the portion legally required.

11. Protected Reports and Trade Secret Immunity

Nothing in this Agreement prohibits either party or any individual from reporting a suspected violation of law, communicating with a government agency or attorney, participating in an investigation, or making another disclosure protected by law. Under 18 U.S.C. 1833(b), an individual is not liable under federal or state trade secret law for disclosing a trade secret in confidence to a government official or attorney solely to report or investigate a suspected legal violation, or in a sealed court filing. An individual suing for retaliation may disclose a trade secret to counsel and use it in the proceeding if filings containing the trade secret are made under seal and disclosure is limited as required by law.

12. Return or Destruction

Upon written request or when discussions end, the Receiving Party will reasonably return or destroy Confidential Information and, if requested, confirm completion in writing. It may retain: (a) one archival copy solely for legal or compliance purposes; and (b) information in routine backup systems that is not readily accessible in the ordinary course, provided all retained information remains protected and is not used for another purpose.



13. Ownership; No License

Each Disclosing Party retains all right, title, and interest in its Confidential Information. No license, ownership interest, assignment, or other intellectual property right is granted except the limited right to use Confidential Information for the Purpose.

14. No Obligation; No Warranty

Neither party is required to disclose information, continue discussions, enter a transaction, purchase services, or award work. Confidential Information is provided "as is" for evaluation. Except as stated in a later signed agreement, the Disclosing Party makes no representation or warranty about completeness, accuracy, merchantability, fitness, noninfringement, or results.

15. Term and Survival

This Agreement remains in effect for the Agreement Term entered on page 1 unless terminated earlier by written notice. The confidentiality and restricted-use obligations apply to each disclosure for the Confidentiality Period entered on page 1. Information qualifying as a trade secret remains protected for as long as it remains a trade secret under applicable law. Sections intended by their nature to survive will survive termination.

16. Remedies

Unauthorized use or disclosure may cause harm that cannot be adequately remedied by money alone. A party may seek appropriate injunctive or equitable relief in addition to other remedies available at law, without waiving any defense or requiring a bond except where required by law.

17. No Publicity

Neither party may use the other party's name, marks, logo, project name, or the existence or status of discussions in advertising, press releases, case studies, social media, or public statements without prior written consent, except as legally required.

18. General

This Agreement is the entire agreement about confidentiality for the Purpose and supersedes prior discussions on that subject. Amendments and waivers must be in a writing signed by authorized representatives. Neither party may assign this Agreement without written consent, except to a successor in a merger, reorganization, or sale of substantially all related assets that assumes the obligations. If a provision is unenforceable, it will be modified to the minimum extent necessary and the remaining provisions continue. Failure to enforce a provision is not a waiver. Headings are for convenience only. A later signed master services agreement, statement of work, data processing agreement, or other contract controls only to the extent it expressly supersedes this Agreement.

**19. GOVERNING LAW AND NOTICES**

Governing law - state or jurisdiction *

Exclusive venue - county and state *

Party A notice address *

Party B notice address *

Party A notice email *

Party B notice email *

20. COUNTERPARTS, ELECTRONIC SIGNATURES, AND ACCEPTANCE

This Agreement may be signed in counterparts and by a legally valid electronic signature. Each counterpart is deemed an original and together they form one agreement. The individuals signing below represent that they are authorized to bind the named party.

PARTY A

Legal name

Authorized signer name *

Title

Signature date *

PARTY B

Legal name

Authorized signer name *

Title

Signature date *

Signature - use a PDF signature tool or print and sign

Signature - use a PDF signature tool or print and sign

Suggested use: Complete the required fields, review the document with counsel, sign through a trusted electronic-signature platform or in ink, and exchange a fully executed copy before substantive confidential discussions. This template is intended for mutual preliminary discussions; a project-specific MSA, SOW, DPA, BAA, security addendum, or other agreement may still be required.