Client Engagement, Data Protection & Responsible AI Policy

Effective date: August 3, 2026 | Public policy version 1.0

Vai-Nova builds practical AI, automation, infrastructure, and cybersecurity systems around real work, human accountability, protected data, and realistic budgets.

Important: This public policy explains Vai-Nova's operating principles. It is not a contract, legal advice, warranty, service-level agreement, privacy notice for a specific system, or substitute for a signed master services agreement, statement of work, nondisclosure agreement, data-processing agreement, or other project document. Project-specific terms control when they differ from this policy.

1. PURPOSE AND SCOPE

- This policy applies to Vai-Nova consulting, discovery, design, development, integration, deployment, infrastructure, cybersecurity, monitoring, support, and research-informed client work.
- Project scope, fees, schedule, deliverables, acceptance criteria, responsibilities, and legal terms are defined in signed project documents.

2. HUMAN LEADERSHIP AND RESPONSIBLE AI

- Human judgment remains accountable. AI may assist with analysis, recommendations, drafting, routing, monitoring, and automation, but sensitive decisions and actions require the approvals defined for the project.
- Vai-Nova will identify material AI limitations, dependencies, and known uncertainty where they affect the intended use.
- AI systems will be tested against the agreed use case before production deployment. Testing does not eliminate all error, risk, or unexpected behavior.
- Vai-Nova will not knowingly design systems intended for unlawful surveillance, deception, unauthorized access, discrimination, harm, or the removal of required human consent or accountability.

3. RIGHT-SIZED, BUDGET-AWARE ENGINEERING

- We begin with the business problem, users, current environment, risk, and available budget - not with the largest possible technology stack.
- Where practical, Vai-Nova may present pilot, essential, professional, advanced, and custom options so a client can start at a responsible level and expand later.
- Proposals separate engineering, hardware, software, licensing, hosting or colocation, backup, support, travel, and third-party costs when those categories apply.
- Our objective is useful adoption and sustainable operation. We do not intentionally oversize new systems merely to increase project value.

4. SECURITY BY DESIGN

- New production systems are designed around current, actively supported hardware and software appropriate to the workload, lifecycle, risk, and budget.
- Security controls may include least-privilege access, multi-factor authentication, network segmentation, secure administration, encrypted communications, logging, monitoring, patch planning, protected backups, restore testing, and documented recovery paths.
- No security architecture can guarantee prevention of every incident. The project scope defines which controls, monitoring levels, response services, and recovery capabilities are included.
- Vai-Nova monitoring is not a 24-hour security operations center unless that service is expressly included in a signed agreement.

5. CLIENT DATA, CONFIDENTIALITY, AND PRIVACY

- The client retains ownership of client data unless a signed agreement states otherwise.
- Vai-Nova will seek the minimum data and access reasonably needed for the work and will use client data only for authorized project purposes.
- Client data will not be used to train a general-purpose model or unrelated system without the client's prior written authorization.
- Vai-Nova does not sell client data. Confidentiality, retention, return, deletion, and incident-notification duties are defined in the applicable agreements.
- Clients should not transmit passwords, private keys, production secrets, protected health information, regulated financial data, or other highly sensitive content through unapproved channels.

6. DEPLOYMENT AND INFRASTRUCTURE CHOICES

- Solutions may be deployed on-premises, on dedicated equipment in an approved colocation facility, in a hybrid architecture, or with approved cloud services.
- The project will identify who owns and administers hardware, accounts, encryption keys, backups, connectivity, licensing, and ongoing operations.
- When hardware is purchased for a client, procurement authority, warranty ownership, shipping, taxes, licensing, return terms, and change procedures should be documented before purchase.

7. PROJECT DEFINITION, DELIVERY, AND CHANGE CONTROL

- A project should define the objective, in-scope and out-of-scope work, deliverables, schedule, dependencies, assumptions, client responsibilities, acceptance criteria, and authorized decision-makers.
- Changes to scope, schedule, deliverables, security requirements, data sources, integrations, or budget may require a written change request or revised statement of work.
- Delays caused by unavailable access, missing data, third-party approvals, procurement, licensing, client decisions, or material changes may affect schedule and cost.
- Deliverables are accepted according to the criteria and review period stated in the signed project documents.

8. INTELLECTUAL PROPERTY AND THIRD-PARTY COMPONENTS

- Each party retains ownership of its pre-existing materials, methods, tools, data, and intellectual property unless a signed agreement states otherwise.
- Ownership or licensing of custom deliverables, reusable components, configurations, documentation, prompts, models, and source code is defined in the statement of work or related agreement.

- Open-source software, commercial software, model licenses, APIs, hosted services, and other third-party components remain subject to their own terms, costs, availability, and security conditions.

9. MONITORING, SUPPORT, AND INCIDENT RESPONSE

- Support hours, response targets, monitoring coverage, escalation paths, maintenance windows, and exclusions must be stated in the project documents.
- When a suspected security incident is reported, Vai-Nova may assist with authorized containment, evidence preservation, log review, recovery planning, and restoration. The client remains responsible for legal, regulatory, insurance, and law-enforcement notifications unless the agreement states otherwise.
- Backups are considered operational only when they are protected, monitored, and periodically tested for recovery within the agreed scope.

10. CLIENT RESPONSIBILITIES

- Clients are responsible for providing accurate project information, authorized access, timely decisions, qualified contacts, required licenses, lawful data use, and a safe working environment for onsite activity.
- Clients must identify regulatory, contractual, privacy, retention, accessibility, and security obligations that apply to their organization and data.
- Clients should maintain independent backups and continuity plans unless Vai-Nova is expressly engaged to design or operate them.

11. TRANSPARENCY, DOCUMENTATION, AND COMMUNICATION

- Vai-Nova aims to explain proposed systems in clear language, including material assumptions, dependencies, human approval points, and operational responsibilities.
- Project documentation may include architecture diagrams, configuration summaries, runbooks, recovery procedures, testing records, acceptance records, and change logs as defined in scope.
- Concerns about privacy, security, data use, deliverables, or project conduct should be raised promptly with the designated project contacts.

12. POLICY UPDATES AND CONTACT

- Vai-Nova may update this public policy as services, standards, law, or operational practices change. The effective date and version will appear on the policy.
- Questions about this policy or a proposed project may be directed to Vai-Nova through the contact information published on the company website.

REFERENCE FRAMEWORKS

This policy is informed by widely used public guidance, including the NIST AI Risk Management Framework, CISA ransomware prevention and response guidance, and common Statement of Work practices reflected in U.S. federal acquisition guidance. These references are not incorporated as contract terms unless a signed agreement expressly says so.

Recommended legal review: Before public launch or use in a binding transaction, Vai-Nova should have qualified counsel review this policy and the company's contract documents for the jurisdictions, services, insurance, and data types involved.