Security at North Idaho AI

Enterprise-Grade Security for AI Solutions

Overview

North Idaho AI designs and implements AI solutions on top of your own Abacus.AI account. You own the Abacus.AI tenant, your data, and your deployed models. We design and operate the AI workflows inside that environment.

Two-Level Security Model

Security is handled at two complementary levels:

- **Platform Security** — Abacus.AI's enterprise-grade security and compliance program provides the foundation.
- **Solution Security** — North Idaho AI designs data flows, access controls, and guardrails tailored to your specific use cases.

This dual approach ensures comprehensive protection from infrastructure through implementation.

Platform Security (Abacus.AI)

We exclusively build on Abacus.AI, an enterprise AI platform with a mature security and compliance program.

Security Program & Governance

Dedicated Security Organization

Abacus.AI maintains a Chief Information Security Officer (CISO) and formal Information Security Committee overseeing all security initiatives.

Risk-Based Defense Program

Implements "defense in depth" methodology with regular risk assessments, vulnerability management, and penetration testing.

External Validation

Undergoes independent external audits and maintains third-party vendor risk management for core subprocessors including AWS.

Data Protection

Encryption Standards

All data is encrypted at rest using AES-256 and in transit via TLS 1.2+ for all network communications.

Multi-Tenant Architecture

Logical isolation between customer accounts ensures complete data separation.

Secure Backup & Recovery

Encrypted backups are stored in geographically distributed locations with regular restore testing.

Access Control

Role-based access control (RBAC) with fine-grained permissions restricts user and service access based on least-privilege principles.

Data Ownership & Usage

Complete Data Ownership

You retain full ownership of your data. Abacus.AI claims no ownership or license rights to customer data.

No AI Training on Customer Data

Your data is never used to train or fine-tune foundational models available to other customers.

Data Residency Options

Configurable data residency available to meet regional compliance requirements.

Secure Deletion

Data retention policies align with your requirements, with secure deletion available on request or end-of-service.

Identity & Access Management

Enterprise SSO Integration

Supports Single Sign-On via SAML and OAuth for enterprise identity providers.

Multi-Factor Authentication

MFA options available for all user accounts to enhance access security.

Comprehensive Audit Logging

Detailed logging of authentication events, data access, and configuration changes.

Least Privilege Enforcement

Principle of least privilege enforced across all platform operations and administrative functions.

Infrastructure Security

Advanced Threat Protection

Web Application Firewall (WAF) and Intrusion Prevention System (IPS) protect against anomalous traffic and common web attacks.

Secure Development Lifecycle

Hardened operating systems, code review processes, automated testing, and OWASP-based security testing.

High Availability Architecture

Designed for 99.95% uptime with automatic failover, encrypted backups, and regular disaster recovery testing.

Compliance & Standards

Abacus.AI maintains compliance with industry-leading security and privacy frameworks:

Security & Audit Certifications	Privacy & Data Protection
SOC 2 Type II	GDPR
ISO 27001	CCPA
ISO 27017	HIPAA-Eligible
ISO 27018	
Encryption & Transport Security	**Industry-Specific Readiness**
TLS 1.2+	PCI DSS
AES-256	FedRAMP
Perfect Forward Secrecy	FISMA

Additional Platform Documentation

For complete technical specifications, architecture diagrams, audit reports, and compliance certifications, please visit:

https://abacus.ai/security

Solution Security (How North Idaho AI Builds)

Where Abacus.AI provides platform-level controls, North Idaho AI is responsible for designing your specific solution architecture—including data flows, feature selection, and implementation guardrails.

Tenant Isolation & Access

Dedicated Tenant Architecture

Each client operates in their own Abacus.AI account with zero data commingling between clients.

Controlled Access Model

North Idaho AI personnel work inside your tenant under accounts and roles that you provision, following least-privilege access principles.

Revocable Permissions

Access is restricted to actively supported projects and environments. You maintain full control and can revoke access at any time.

Data Classification & Minimization

Collaborative Classification

We work with your team to classify data by sensitivity level (internal, confidential, regulated such as PII/PHI/PCI).

Minimum Necessary Standard

AI workflows are designed to use only the minimum data required for each specific use case.

Privacy-Enhancing Techniques

Where appropriate, we implement masking, redaction, tokenization, or pseudonymization for sensitive fields while preserving analytical value.

AI Guardrails & Controls

Safe Use Policies

We help define internal "safe use of AI" rules to prevent exposure of secrets, raw cardholder data, or classified content.

Pre-Processing Safeguards

When required, implement pre-processing to remove or redact PII/PHI from documents before indexing.

Role-Based Scoping

Project and role-based access scopes ensure different user groups only access data they're authorized to view.

Segmented Retrieval

Retrieval-augmented generation (RAG) pipelines respect existing data segmentation by business unit, region, or client.

Logging & Data Lifecycle

Usage Monitoring

We encourage comprehensive logging of assistant usage, data source access, and AI project configuration changes.

End-of-Engagement Cleanup

At engagement completion, we can help archive or securely delete datasets, indexes, and models created during implementation.

Policy Alignment

Data retention and deletion practices align with your existing corporate policies and compliance requirements.

Industries & Use Cases

North Idaho AI and Abacus.AI are designed for security-conscious and regulated organizations across multiple industries.

Healthcare & Life Sciences

HIPAA-aligned architectures where Protected Health Information (PHI) is handled only when necessary, under strict controls and data minimization principles.

Financial Services & Fintech

Implementations aligned with SOC 2 and ISO 27001 expectations for internal copilots, analytics platforms, and customer support tools.

Retail & E-Commerce

AI solutions that integrate with existing PCI-compliant systems using tokenization and minimal cardholder data exposure.

B2B SaaS & Professional Services

Confidentiality-sensitive knowledge assistants and copilots with clear data separation by client, region, or practice area.

Working With Your Security Team

We regularly collaborate with Chief Information Security Officers (CISOs), security architects, and compliance teams throughout AI adoption initiatives.

What We Provide

Architecture & Data Flow Documentation

High-level architecture diagrams and data-flow documentation tailored to your specific use cases.

Platform Clarification

Detailed explanations of how Abacus.AI handles encryption, access control, logging, data residency, and compliance.

Governance Guidance

- Assistance developing internal guardrails and acceptable-use policies for AI adoption across your organization.

Schedule a Security Discussion

To discuss your specific security requirements, compliance obligations, or technical architecture questions:

- Email: john@northidahoai.com
- Phone: (208) 732-2337
- Website: https://northidahoai.com/contact
- Security Page: https://northidahoai.com/security

About North Idaho AI

North Idaho AI brings enterprise-level AI capabilities to small and mid-sized businesses in North Idaho and the Inland Northwest. We specialize in AI consulting, implementation, and AI-native websites for businesses in Coeur d'Alene, Sandpoint, and Spokane.

Our Approach

We don't just consult—we build, deploy, and deliver working AI solutions that generate measurable ROI from day one.

Key Differentiators

Production Systems, Not Strategies

We deliver deployed, working systems rather than strategy documents and recommendations.

Rapid Implementation

Production-ready implementations delivered in weeks, not quarters.

Your Infrastructure

Your data and deployed models remain in your own Abacus.AI tenant under your control.

Security-First Design

Enterprise-grade security architecture from day one, not as an afterthought.

Local Focus

Serving businesses in Coeur d'Alene, Sandpoint, and Spokane with onsite visits available.

North Idaho AI
Coeur d'Alene, Idaho
Contact: john@northidahoai.com | (208) 732-2337
Website: www.northidahoai.com

Document Version 1.0 | December 2025