



AlgoVerde Platform Security



An Overview

AlgoVerde transforms product development and market intelligence with cutting-edge AI solutions. **Trusted by Fortune 500 companies**, our platform enables businesses to ideate, test, and validate product concepts faster and with greater confidence.

AlgoVerde was built with robust security as a top priority. **Security is paramount** both at the application and user levels.

Cloud-Based Deployment

We host AlgoVerde on Amazon Web Services (AWS) and follow the same standards and best practices used by leading enterprise applications, including Salesforce and Microsoft 365. Nothing runs from our corporate offices, and we don't store customer data on our premises.

User Authentication

We require secure, unique login credentials for every user to protect your data. Only people you specifically invite can access the platform. This gives you tight control over who uses the system and prevents unauthorized access.

Role-Based Access

You can define exactly which users have access to what within each innovation space. This role-based system lets you control who sees specific workspaces, keeping sensitive information secure and confidential.

Firewall

We use multiple layers of firewall protection, including AWS firewalls and our own AlgoVerde-specific firewalls. We can also configure things so all your data stays within your company's internal firewall, giving you an extra layer of control and security.

Certifications

AlgoVerde has obtained **SOC2 Type 1 SOC2** and **Type 2 certifications** and is in the process of obtaining **ISO27001 certification**.



Data Security

All internal work, including prompts and responses, stays completely contained within your secure customer instance.

We protect your data with several key approaches:

Dedicated Instances

Each customer gets their own dedicated software instance, like having your own isolated workspace. This means your data never gets mixed with other customers' data.

Data Obfuscation

We use an embedding integration process that only keeps the obfuscated (tokenized) version of your data on our platform. This ensures both confidentiality and security.

Data Encryption

We encrypt everything – both disk storage and databases. AWS manages and securely stores the encryption keys, and our personnel can't access them. We log and monitor all key usage to catch any unusual activity. This protects against unauthorized access, theft, and data breaches.

Data Retention Policy

We only keep your data for the length of our agreement. After that, we follow our Data Retention Policy unless you ask us in writing to delete everything. AWS handles proper sanitization of disks and physical media. We also sanitize employee laptops before reusing or disposing of them.

AV GenAI Personas

Your GenAI Personas belong to your company and will never be shared with anyone beyond the permissions you set.

AV Workflows

The custom Business Processes we develop for your deployment get the same level of security protection as everything else.

Integration with External AI Models

AlgoVerde deploys a mix of commercial and Open Source LLMs. All are accessed via **proprietary APIs**. The platform defaults to the best available LLM for each task, though users can change the model selection when needed to align with internal policies or preferences. When external models are used, requests are routed through **enterprise-grade APIs** operating under standard **enterprise SLAs and governance controls**.

All deployments are housed on a **dedicated instance**, with access permissions dictated by team members. **Data is never shared** across customer instances and never used to train any models (we do not have proprietary LLMs).

We can integrate your company's **private instance** of ChatGPT, Gemini, Claude, or any other proprietary model.

Confidentiality Agreement with Employees

Security is everyone's responsibility. No AlgoVerde employee can access your Innovation Space or proprietary data unless you specifically invite them. **All employees and contractors must sign a confidentiality agreement**, the employee handbook, and **our security policies**.

Customer's Responsibilities

While we handle the vast majority of security controls to protect your data and the application, **you're responsible for securing your user accounts**. This includes creating strong passwords, managing user accounts and permissions, and disabling accounts when needed. **You're also responsible for determining what data is appropriate to enter into the application.**

