AlgoVerde Platform Security - an Overview

AlgoVerde (AV) is the future of enterprise innovation: a cutting-edge GenAI Platform that **empowers businesses to achieve breakthrough innovation** with the transformative power of Generative AI. AlgoVerde increases team productivity and fosters collaboration.

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

Cloud-Based Deployment

AV is hosted on Amazon Web Services (AWS) and it adheres to the latest standards and best practices followed by top-tier enterprise applications, such as Salesforce and Microsoft 365. AlgoVerde corporate offices do not host any component of the infrastructure or store customer data.

User Authentication

To ensure the security and integrity of data, AV mandates the creation of user profiles with secure login credentials. Only individuals who have been invited to the platform and are authorized have access to AV.

Role-Based Access

Within each innovation space, AV enables customers to precisely define user roles and permissions. This empowers customers to exercise granular control over which users have access to specific workspaces, guaranteeing the security and confidentiality of sensitive information.

Firewall

While AV is secured by multiple firewalls (including AWS firewalls and AV's physical firewalls), it is also possible to configure AV so that a user's data resides exclusively inside a company's firewall.

Certifications

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

Data **Security**

AV is deeply committed to safeguarding the integrity and confidentiality of customer data.
Our approach to data security is based on:

- **Dedicated Instances:** Each customer is provided with a dedicated software instance, functioning as an isolated workspace. This ensures that no customer data is ever shared with other customers. All internal work, including prompts and responses, is fully contained within a secure customer instance.

- **Data Obfuscation:** Using an embedding integration process, only the obfuscated (tokenized) representation of the data is maintained on the AV platform,ensuring both data confidentiality and security.

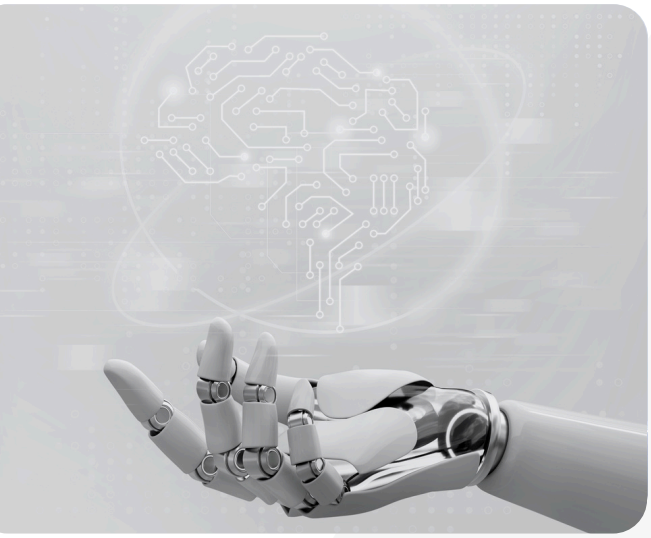
- **Data Encryption:** The data encryption includes disk encryption and database encryption. Encryption keys are managed by and stored securely in AWS. AV personnel do not have access to the encryption keys. All key usage is logged and monitored for anomalous activity.This process provides protection against unauthorized access, theft, and data breaches.

- **Data Retention Policy:** AV retains customer data only for the duration of the agreement. Following termination, data is retained in accordance with AV's Data Retention Policy, unless it receives a written data deletion request. AWS is responsible for ensuring the proper sanitization of disks and physical media. AV sanitizes employee laptops prior to reuse or disposal.

- **AV GenAI Twins:** GenAI Twins are proprietary to a company and will never be shared with anybody beyond the permissions dictated by that company.

- **AV Workflows:** As with all other data, the AlgoVerde Pathways are protected by the same level of security.

Integration with **External AI Models**



The AV platform is designed to use a mix of Open Source LLMs (private instances) and be extended with external AI models such as ChatGPT, Claude, and Gemini or other models developed by your company. In case these models are used, AV notifies users of any possible security concerns and utilizes the maximum security measures allowed by these third-party models. It can also integrate a company's private instance of ChatGPT, Gemini, Claude, or other.

Confidentiality Agreement with **Employees**

Security of the AV environment is the shared responsibility of all AV employees and contractors who have access to AV's information systems. No AV employee is able to access a company's Innovation Space or proprietary data unless specifically invited by the company itself. Employees and contractors must also sign a confidentiality agreement, the employee handbook, and AV's security policies.

Customer's **Responsibilities**

While AV is responsible for the vast majority of the security controls implemented to secure customer data and the application, our customers are responsible for securing their user accounts. This includes creating strong passwords, provisioning user accounts and permissions, and disabling accounts as needed. Additionally, customers are responsible for determining the appropriateness of the data entered into the application.

Frequently Asked **Questions**

What is AlgoVerde?
AlgoVerde (AV) is a cutting-edge SaaS Innovation Platform, empowering businesses with the transformative power of Generative AI to drive breakthrough innovations.

Can AV be integrated with other Generative AI models?
At the customer's request, the AV platform can be integrated with third-party models (e.g. Open AI ChatGPT, Gemini, Claude, etc.) and/ or with the customer's specific models.

How is AV deployed?
AV is a cloud-based solution. For privacy and security reasons, AV is structured in individual instances (one instance for each customer).

How is our innovation work security stored and managed?
The AV platform is compliant with any and all security standards guaranteed by industry-leading cloud service providers which are certified for security data storage.

Is my company data shared with other AV customers?
No, your company data is never shared with anybody. It is stored in a private instance dedicated to your company and only accessible to users identified by your company.

Is my company data used to train AV models?
No, your company data is not used to train any AV models. Upon request, we can fine-tune your private AV models to improve the outcome of the innovation process. Your private, fine-tuned models are never shared with other customers.

What certifications does AlgoVerde hold?
AlgoVerde is finalizing the SOC 2 type 2 and ISO 27001 certifications.

AlgoVerde

IT - Frequently Asked **Questions**

Organizational Security Measures

Area	Question	Answer
Privacy Organizational Model	Is there a Privacy Organizational Model?	Yes
Persons Authorized to Process	List the Categories of Persons Authorized for Processing	Algoverde SW Engineers only
	Are there any official instructions and appointments of the persons authorized for processing?	Yes
	Are the Authorized Persons for the processing of confidential data at high risk bound by specific confidentiality clauses (under their employment contract or other legal act)?	Yes
	Is there an internal Regulation for the use of company information tools and services?	Yes
	Are there any regular awareness campaigns or specific Privacy and Security training initiatives for company employees who process confidential data?	Yes
Other Data Processors	Who is the Supplier used for the processing in question? Indicate the list of Suppliers	Amazon Web Services (AWS)
	Is there any official appointment with "other data processors" (i.e. Sub-Processors)?	No
	Is the staff aware of the privacy regulations in force/are they properly trained in this regard?	Yes

Organizational Security Measures

Area	Question	Answer
Other Data Processors	Do you request your suppliers/subcontractors (if permitted by the contract) of ICT services to adopt appropriate security practices along the supply chain?	All our subcontractors have the same level of security practices
	Is the Sub-Processor in possession of certifications?	Amazon AWS is in possession of the following certificates and more: • ISO 9001:2008 • ISO/IEC 27001:2013 • ISO/IEC 27017 • ISO/IEC 27018:2014 • SOC 2 Full list available here
Data Retention	Indicate how long personal data is stored in both digital and paper format	Service duration only
	Is There a protocol for removing Confidential Data from Platforms/Applications, according to the indications of the Customer?	Yes
Data Breach	Has the company implemented an Incident Response Plan with detailed procedures to ensure an effective and proper response to incidents or data breaches?	Yes

IT Security Measures

Area	Question	Answer
Safety Standards	Is there any procedure in place to ensure the confidentiality, integrity and availability of the information? If so, please indicate which ones	Yes. The following procedures are in in place: - Intrusion prevention - Intrusion detection - Disk encryption - Data scrambling - Access via SSL authentication only

IT Security Measures

Area	Question	Answer
Safety Standards	Are standards, certifications adopted?	All the digital infrastructure and customer data are hosted in AWS. The hosting provider is ISO/IEC 27018 certified
	Are there sufficient digital data protection measures in place (e.g. encryption, etc.) to protect the information in case of remote access?	All the remote access are SSL/TLS encrypted
	Are any special measures used according to the level of criticality of the personal data processed? If so, which ones?	All the data are managed as the maximum level of security
Authentication	Are Identity and Access Management procedures and tools used? Even with multiple factors (strong authentication)?	Yes, 2FA (available on-demand)
Password Policy	Has the company implemented a password policy? Is the access control system able to detect and not allow the use of passwords that do not respect a certain degree of complexity?	Yes
	Are the log files marked with the date and time and protected against any manipulation and unauthorised access?	Yes
User Profiles	In order to have access to the Platforms/Applications, has the supplier developed restrictive profiles in relation to Personal Data, which allow access only to the data necessary to carry out its activities (principle of data minimisation)?	Yes
Data Communication Networks	Is network traffic monitored and controlled via firewall and intrusion detection systems?	Yes all the communications are encrypted using SSL/TLS

IT Security Measures

Area	Question	Answer
Data Communication Networks	Is there any safe management of data communication, e.g. based on PKI? Are VPNs used? Is Router security guaranteed?	Yes
	Are appropriate communication encryption technologies used, sufficient to ensure the security of the information exchanged?	Yes
Antivirus	Are there antivirus software, even on all the endpoints connected to the Platforms/Applications?	Yes
Backup	Are backup procedures for systems containing and processing data and information planned, adopted and documented?	Yes
	Are backups being programmed for versioning? If yes, for how much time/days?	Daily and weekly
	Are periodic checks (automatic and manual) carried out on the integrity of backup archives and backup media? If so, how often?	Yes, every 6 months
Disaster Recovery	Has the company implemented Disaster Recovery processes for the premises? Is there any Disaster Recovery Test formalized and performed on an annual basis?	Yes
SOC & IDS	Are there automatic IPS (Intrusion Prevention System) systems that track and attempt to report and block malicious activity?	Yes
	Are there automatic IDS (Intrusion Detection System) systems for the detection of unauthorized access and intrusion?	Yes
	Are Vulnerability Assessment and Penetration Tests carried out in your area?	Yes

IT Security Measures

Area	Question	Answer
Cloud Computing	Are specific measures adopted for data protection in the Cloud? If so, which ones?	Check here
Change Management	Is there a periodic update of the platform (security patch)?	Yes

Physical Safety Measures

Area	Question	Answer
Physical Access of the Data Processor	Do you use a badge or other security systems to access the buildings/offices in which the data are stored?	Yes
	Is the physical perimeter of the IT system infrastructure accessible only to authorized personnel?	Yes
	Are there access control systems and anti-burglary measures, also through security guards?	Yes
Damage Prevention to Structures	Are there any safety measures available in the company to prevent infrastructural damage (e.g. caused by smoke and/or flames)?	Yes
BMS	Is the building that hosts the Information System equipped with a BMS (Building Management Systems)?	Yes
	Is there a UPS (Uninterruptible Power Supply) Group?	Yes