ABACUS.AI

Information Security And Compliance Paper

Abacus.AI Security Posture

Abacus.AI has implemented comprehensive security controls across every aspect of product development, hosting, and delivery life cycles. These security controls were developed and implemented with the singular goal of safeguarding our customer's data using best-in-class industry frameworks and practices. This paper documents those controls along the following dimensions:

- Administrative & Organizational controls
- Software development life cycle
- Infrastructure & Operational controls
- Standards & Regulatory Compliance

Product offering

Abacus.AI is a cloud software as a service (SaaS) offering that runs in public or private cloud infrastructure to help enterprises develop and operate sophisticated Artificial Intelligence (AI) deep-learning models across a variety of enterprise use-cases ranging from Recommendation Engines to Forecasting to Anomaly detection. For a comprehensive description of our product offerings please refer to https://Abacus.AI.

Administrative & Organizational controls

a. Employee Background Checks:

   Abacus.AI performs background checks for all employees who have access to customer data.

b. Security Awareness Training:

All employees undergo security training before accessing any customer data. All technical employees also receive a security newsletter every week. The employees are trained on and are made aware of email scams, hoaxes, malware detection, phishing attacks, social networking dangers, safe internet habits, clean desk practice, and how to handle and secure sensitive data.

c. Data Policies

Comprehensive data classification, access policies are in place to ensure that customer data is only accessed on a need-to-know basis governed by a principle of least privileged access. Abacus.AI's customers continue to own the data they use on the product to build models and only provide temporary read-only access to the data. Abacus.AI will only process the data to fulfill our contractual obligations and not for any other purpose such as scanning for advertisements or selling to third parties. we do not scan it for advertisements nor sell it to third parties. Furthermore, if customers delete their data, we commit to deleting it from our systems within 15 days.

Software development life cycle

a. Source Code Policies

Abacus.AI's source code is stored in a central repository where both current and past versions of the service are auditable. The infrastructure is configured to require that a service's binaries be built from specific reviewed, checked in, and tested source code. Code

reviews require inspection and approval from at least one engineer other than the author, and the system enforces that code modifications to any system must be approved by the owners of that system. These requirements limit the ability of an insider or adversary to make malicious modifications to source code and also provide a forensic trail from the service back to its source.

b. Static Code Analysis

Static code analysis tools are in place to ensure that secure programming guidelines are adhered to and violations get flagged and alerted.

c. Continuous Integration and Deployment

Continuous integration and deployment pipelines have been built to execute comprehensive quality checks on every code modification and successful test execution is required before deployment to production.

Infrastructure & Operational controls

a. Access Control & Two-Factor Authentication

Comprehensive Role-based access controls have been implemented across the entire network stack starting from internal IT systems to production infrastructure governed by the principle of least privilege. Two-Factor authentication has been deployed across all the infrastructure. The Two-Factor authentication prevents phishing attempts and requires employees to use a username and password as well as an authorization code that is sent to their mobile device. This ensures that there is an additional layer of security on all our systems.

b. Network Infrastructure

Multi-tiered network topology has been implemented to reduce the surface area of exposure. Network Access Control Lists and firewalls limit network traffic between the network layers. Virtual private networks are in place for internal access. Strict compute isolation is in place for different environments and customers. Strict data isolation is in place along with dedicated encryption keys for customer data.

c. Securing Customer Data - Encryption at rest

All Customer Data is always stored in secure locked-down object storage infrastructure (AWS, GCP, Azure). All data is encrypted at rest. Access to the buckets is restricted to the few employees that are working on the customer's data. Customer-specific encryption keys are generated for each customer. This key management service supports automatic key rotation and provides extensive audit logs. In addition, AWS Macie is enabled on the buckets to ensure that there is 24/7 monitoring, automated detection of anomalies, and alerting of any unauthorized access.

d. Data Isolation

To keep data private and secure, Abacus.AI logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of our employees have access to customer data. Abacus.AI employees, access rights, and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Abacus.AI employees are only granted a limited set of default permissions to access company resources, such as employee email and Abacus.AI's internal employee portal. Requests for additional access follow a formal process that

involves a request and an approval from a data or system owner.

e. Physical Infrastructure

We use AWS data centers for data storage and all computation. AWS data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Their data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. To keep things running 24/7 and ensure uninterrupted services, AWS data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment help prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

f. Monitoring

Abacus.AI uses security monitoring services such as AWS Macie (https://aws.amazon.com/macie/) to continuously monitor data access

activity for anomalies and generates detailed alerts when it detects the risk of unauthorized access or inadvertent data leaks. All customer data is monitored for access activity 24/7 and all access is logged for auditing purposes. Our security engineers monitor all accesses on a regular basis and immediately react to alerts generated by the automated monitoring system.

g. Incident Management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. If an incident involves customer information, Abacus.AI will inform the customer and support investigative efforts via our support team.

h. Vulnerability testing

Periodic external 3rd party vulnerability scans are performed to identify and remediate any vulnerabilities in our software and serving infrastructure across our external interfaces.

Standards & Regulatory Compliance

a. Security Standards: CIS v1.2.0 & PCI DSS 3.2.1

Abacus.AI systems are fully compliant with CIS 1.2.0 and PCI DSS v3.2.1 guidelines. Automated security alerts are in place to identify and

remediate any deviations from the standards.

b. GDPR

Abacus.AI systems are fully compliant with GDPR guidelines around data protection and privacy. Any reporting or deletion requirements around GDPR will be honored within 15 days.

c. CCPA

Abacus.AI systems are fully compliant with CCPA guidelines around data protection and privacy. Any reporting or deletion requirements around CCPA will be honored within 15 days.

d. HIPAA

Abacus.AI systems are fully compliant with HIPAA guidelines and can enter into a Business Associate Agreement if necessary.

Conclusion

Abacus.AI products and infrastructure has been designed and built with cloud-first architectural principles with the singular goal of safeguarding our customer's data using best-in-class industry frameworks and practices. The protection of our customers' data is a primary design consideration for all of Abacus.AI's infrastructure, products, and personnel operations.