Adaviv Security and Data Privacy Policy

Adaviv is committed to protecting the confidentiality, integrity, and availability of customer data. This Security Policy outlines the measures we take to safeguard data and systems. This policy applies to all Adaviv employees, contractors, and third-party service providers who handle customer data. Our security program is designed with industry best practices in mind, including those outlined in the NIST Cybersecurity Framework and SOC 2.

Security Framework

Network Security	**Cloud Reliance:** Adaviv primarily leverages the security infrastructure provided by Amazon Web Services (AWS) and Google Cloud Platform (GCP). **AWS/GCP Practices:** Adaviv utilizes security features such as VPCs, security groups, IAM for fine-grained access control, and managed services. **Microservices Architecture:** Microservices and databases communicate over private networks, minimizing public internet exposure.
Data Security & Privacy	**Data Classification:** Adaviv classifies data based on sensitivity (e.g., confidential, public) to enforce appropriate security controls. **Encryption:** Data is encrypted in transit and at rest using industry-standard algorithms and services provided by AWS and GCP. **Access Controls:** Access to sensitive data is strictly controlled based on the principle of least privilege, leveraging AWS IAM and GCP IAM roles and policies. **Secrets Management:** Secrets (API keys, database credentials, etc.) are managed using AWS Secrets Manager with encryption with rotating keys policy, avoiding hard-coded values. **Authentication:** API authentication is managed securely using Google Identity Platform and AWS Cognito and Google Cloud Authentication, employing short-lived JWT tokens. Our API authentication design enforces stringent access controls, implementing granular read/write privileges akin to row-level security. Tokens are user-specific and tied to designated service accounts, ensuring that requests are authorized only when the service account in the API call aligns with the user token's associated account. **Control Status:** The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. **Customer data deleted upon leaving:** The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. **Data classification policy established:** The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
Compliance with Privacy Laws and Specific Protections for Personal Data	Adaviv is committed to safeguarding the privacy and security of our users' personal data, in alignment with applicable privacy laws, including the California Consumer Privacy Act (CCPA). We recognize the importance of privacy and have implemented measures to protect the personal information we collect, including user names, professional emails, and mobile numbers provided by users who opt-in to receive notifications, reports, and emails related to Adaviv services. **Personal Data Collection and Use**: Personal data collected is limited to what is necessary for providing Adaviv services and is used strictly in accordance with user consent. **Encryption and Security:** All personal data, including names, emails, and mobile numbers, is encrypted in transit and at rest, utilizing the robust security infrastructure. **Access Control:** Access to personal data is restricted to authorized personnel only, based on the principle of least privilege, and is controlled through fine-grained access policies such as AWS IAM and GCP IAM roles. **Data Retention and Deletion:** Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected. Upon termination of services or at the user's request, personal data is securely deleted from our systems in accordance with our documented retention and disposal procedures. **Compliance Measures:** Adaviv adheres to a rigorous data classification policy, ensuring that all data, especially personal information, is appropriately secured and managed. We are committed to continuous monitoring and improvement of our security practices, staying abreast of changes in technology, legal requirements, and best practices for data protection. Our incident response plan includes specific provisions for addressing security breaches, including timely notification to affected individuals in compliance with the CCPA and other applicable regulations.

Incident Response	**Detection:** Adaviv monitors security events through AWS CloudWatch, AWS CloudTrail, and GCP Cloud Logging. Tools and processes are in place for identifying suspicious activity. **Response Procedures:** Adaviv has defined procedures for containment, investigation, and reporting of security incidents. **Customer Notification:** Adaviv's incident response plan includes provisions for notifying customers of breaches in accordance with contractual obligations and applicable regulations.
Vulnerability Management	**Patching:** Adaviv follows a patching process for promptly applying security updates to software and systems, leveraging managed services from AWS and GCP where applicable. **Scanning:** Adaviv uses vulnerability scanning tools and services on a regular basis to identify potential weaknesses. **Audit Cadence:** Regular third-party audits and internal vulnerability scans are conducted to identify and address potential security risks.
Review and Updates	Adaviv reviews and updates this Security Policy on a regular basis to reflect changes in technology, security best practices, and legal requirements.