TIFIN AMP

Customer Security Overview

TIFIN AMP is committed to protecting its employees, partners, clients/customers, and the company itself from damaging acts, either malicious or unintentional in nature. This includes the implementation of policies, standards, controls, and procedures to ensure the Confidentiality, Integrity, and Availability of systems and data according to their risk level.

The TIFIN AMP security program and policies are developed on the principles that (1) security is everyone's responsibility and (2) self-management is best encouraged by rewarding the right behaviors.

TIFIN AMP hosts all its software in Amazon Web Services (AWS) facilities in the USA. Amazon provides an extensive list of compliance and regulatory assurances, including SOC II and ISO 27001. See Amazon’s compliance and security documents for more detailed information.

All of TIFIN AMP’s servers are located within TIFIN AMP’s own virtual private cloud (VPC), protected by restricted security groups.

TIFIN AMP conducts application and network penetration testing by a third-party at least annually.

TIFIN AMP logins require strong passwords. User passwords are salted, irreversibly hashed, and stored in a world-class identity management solution. In addition, TIFIN AMP has deployed controls to flag high-risk logins. Audit logging lets administrators see when users last logged in and when a password last changed.

All connections that carry sensitive information are encrypted using TLS, and any attempt to connect over HTTP is redirected to HTTPS. All customer data is encrypted in rest and in transit.

Data access and authorizations are provided on a need-to-know basis and based on the principle of least privilege. Access to the AWS production system is restricted to authorized personnel and is carried out using VPN with MFA (Multi-Factor Authentication).

All access to TIFIN AMP applications is logged and audited, in which logs are kept for at least one year.

TIFIN AMP maintains a formal incident response plan for major events.

TIFIN AMP maintains security policies that are maintained, communicated, and approved by management to ensure everyone clearly knows their security responsibilities.

TIFIN AMP development and testing environments are separate from the production environment.

TIFIN AMP's employee hiring process includes background screening.

TIFIN AMP maintains and publishes a privacy policy on how we use and store data which is updated at least annually.

Vulnerability Disclosure Process – TIFIN AMP considers privacy and security to be core functions of our platform. Earning and keeping the trust of our customers is our top priority, so we hold ourselves to the highest privacy and security standards. If you have discovered a security or privacy issue that you believe we should know about, we would love to hear from you. You can contact us and submit a vulnerability via security@tifin.com.