



SECURITY BRIEF



THE LEADING SaaS SOLUTION FOR MANAGING FX CURRENCY RISK

As the data experts, we pride ourselves on our security and take every precaution to ensure data is safe. FiREapps security protocols have been approved by hundreds of top global IT and security organizations. We invest heavily in the data security of our applications by employing current standards and incorporating relevant security measures and compliance into our infrastructure and internal processes.

PRODUCT SECURITY

DATA ENCRYPTED IN MOTION & AT REST

All application data, user IDs, and passwords are protected and encrypted using 256-bit AES in motion and at rest within FiREapps full suite of products.

APPLICATION-ONLY ACCESS

FiREapps system is divided into layers that separate data from the application. Individual users only have access to the application layer, ensuring no one can access or alter data.

ROLE-LEVEL ACCESS & IDLE DISCONNECT

Each user is assigned a specific role and set of permissions that control what they can see and the features available. Additionally, the system can detect idle connections and will automatically terminate the session after a period of time.

COMPLETE AUDIT TRAIL

FiREapps maintains a complete audit trail to track who made entries when, referencing each transaction by the user login details.

PREVENTION OF MALICIOUS ACTS

FiREapps takes proactive measures to ensure the application is safe from internet attacks. Every server is behind a firewall to prevent users from accessing them without the proper protocols and methods. In addition to the firewalls, FiREapps has an extra level of protection around the production databases, allowing access only from specific hosts.

CONTINUOUS MONITORING

FiREapps employs port scans and network intrusion detection systems (NIDS) to identify possible network vulnerabilities. Unauthorized attempts to access FiREapps data center are blocked and logged for further investigation.

DATA BACK-UP

All FiREapps client data is automatically backed up daily and encrypted. Backups are transferred to globally-redundant cloud storage facilities.

COMPLIANCE

In order to ensure the safety and security of our clients' data, FiREapps has voluntarily implemented information security programs to govern the management and handling of all information assets within our solutions.

FiREapps actively works with clients to continually meet security standards – we perform audits and reviews of our information security controls, including certified ISO 27001 and SSAE 18 SOC 1 Type 2 standards. These audits require FiREapps to regularly demonstrate continued effectiveness of controls.

SSAE 18 AUDIT

SSAE 18/ISAE 3402 is defined and governed by the American Institute of Certified Public Accountants and the International Accounting Standards Board to provide assurance to a company's clients about the effectiveness of the controls within the service organization.

FiREapps has been undergoing SSAE 18 SOC 1 Type 2 audits (previously SAS 70 and SSAE 16) since 2009. With the recent adoption of SSAE 18, audited firms are required to conduct additional in-depth reviews of critical service providers and mapping of their User Control Considerations to FiREapps' own controls, ensuring consistency and completeness of controls across organizations.

ISO 27001 AUDIT

ISO 27001 is an internationally recognized certification process that verifies the implementation and effectiveness of 114 information security controls as defined by the International Organization for Standards (ISO). ISO 27001 certification requires organizations to demonstrate a working Information Security Management System (ISMS) and is mitigating risk through the implementation of controls by processes, politics or systems across departments and staff. The ISMS is a complete system for assuring information security. Organizations achieving this standard have to demonstrate a solid system for managing information security.

FiREapps has undergone ISO 27001 audits since 2015 and in order to maintain certification, goes through biannual audits to review the processes and controls of the ISMS. The first audit – the internal audit – requires FiREapps to engage an independent, certified third-party auditor to conduct a review. The second FiREapps audit – the certification audit – is conducted by the British Standards Institute. The ISMS includes risk assessment and treatment for the areas of HR, access control, physical security, application development and disaster recovery. FiREapps confirms its commitment to this standard by looking to continually improve in the areas of risk assessment quantification and treatment methodology, as well as undergoing regular reviews of objectives, controls and ISMS performance.



INFORMATION PRIVACY

FiREapps complies with the EU-US and Swiss-US Privacy Shield Requirements for the protection and safeguarding of personally identifiable information (PII). This program compliance ensures FiREapps has implemented the appropriate frameworks for management of PII – a special classification of information assets. While FiREapps use of PII is limited to identity management, we nonetheless elevate this class of data to ensure the safety and security of our clients' information.

OTHER SECURITY CONSIDERATIONS

As an integral component of FiREapps strategic direction to move away from collocated services into the public cloud, FiREapps security profile increases by several orders of magnitude. In addition to the resources brought to focus by FiREapps, the resources of organizations like Microsoft and Amazon are being utilized to continually ensure the security of clients' information.

GENERAL DATA PROTECTION REGULATION (GDPR)

FiREapps has completed a third-party readiness assessment for complying with the provisions of GDPR. In addition, appropriate procedures and practices have been adopted to ensure proper handling and processing of personal data in accordance with GDPR requirements.

SERVICE DELIVERY INFRASTRUCTURE & CONTROLS:

- ▶ ISO/IEC 27001:2013 certified Information Security Management System
- ▶ Annual SSAE 18 SOC 1 Type 2 and Type 1 Audits
- ▶ 24 x 7 operations monitoring
- ▶ Multi-factor authentication for administrators
- ▶ EU-US and Swiss-US Privacy Shield certified
- ▶ AES-256 encryption methodologies for data in motion and at rest
- ▶ Third-party penetration testing
- ▶ Tiered support structure and problem resolution processes
- ▶ Multi-tenant with application layer logical separation and single tenant configurations
- ▶ Online support network
- ▶ Internet firewalls and additional levels of access control around the production databases
- ▶ Application layer separation from data with application-only access
- ▶ Role-level access and idle disconnect
- ▶ IP Whitelisting, guaranteeing client access from only specific internet addresses
- ▶ Continual monitoring through intrusion prevention systems
- ▶ A complete audit trail in application and data back-up
- ▶ Application hosting in world-class cloud service providers



FiREapps is the leading provider of cloud-based enterprise currency management (ECM) solutions for currency exposure management and enterprise currency analytics. Established in 2005, FiREapps developed the first solution to automate foreign exchange exposure management for multinational companies. Today, the company provides automated solutions to support the analysis and management of currency exposure, as well as the assessment and reporting of how currencies can impact corporate financial performance.

FiREapps is headquartered in Scottsdale, Arizona, with offices in Portland, London and Frankfurt.

For more information, visit www.fireapps.com/ or call +1 866-928-FIRE (3473).