

# Technology Overview: IT Security, Privacy & Compliance

## Data protection is essential for your organization. Here's how SAI Global will help.

SAI Global delivers integrated Risk Management (IRM) solutions that are scalable, secure, reliable and redundant. We deploy SaaS applications architected with the highest compliance and uptime standards. Our hosting is fully virutalized, engineered for redundancy and reliability, to avoid any single point of failure.

For customers using one of our on-premise offerings, we are no less diligent. We develop our applications and services with the utmost reliability and uptime in mind.

As a recognized provider of IRM solutions, we continuously stress the need for confidentiality, integrity and availability of your data. We constantly scan and monitor our systems to ensure your sensitive risk and compliance data is safe. Rest assured that SAI has taken the security and compliance needs of our global clients seriously.

"SAI Global's customers entrust us with sensitive data and we take that responsibility very seriously. SAI Global invests heavily in highly skilled personnel and in thorough security processes to protect it."

*Peter Granat, Chief Executive Officer of SAi Global*

SAI Global maintains a comprehensive security and compliance program to mitigate risks for our clients beginning with the design of our systems, followed up by ongoing oversight and monitoring.

## SECURITY AND COMPLIANCE

SAI Global has implemented the following compliance certifications and procedures to harden our platform. Copies of certifications, reports and agreements can be obtained by request.

- Detailed and continuous vulnerability scanning, virus scanning and intrusion prevention
- All systems are housed in IS027001 certified data centers owned and managed by global leaders
- All systems are operated and managed by the SAI Global Hosting Service which is ISO27001:2013 certified globally
- SOC2 Type 2 report (SSAE18)*
- Independent Practitioner's Report on the information security program for the Integrated Risk Management Solutions (SAI360) System Related to HIPAA and HITECH

*The 2018 SOC2 examination scope was on the SAI360 Integrated Risk Management Platform as hosted in the Americas. The July 2019, examination scope has been extended to include the SAI360 Integrated Risk Platforms hosted in the Australia and the UK Data Centers, and operating in AWS (Germany). The 2019 Reports will also expand to include the SOC1 Type 2 (SSAE2018) and ISAE3402 Reports.

## DATA CENTERS

SAI Global runs its applications in regionalized data centers, including Sydney, Atlanta, and Milton Keynes. The key tenets of our data centers are:

- Data center service provider is responsible for physical and environmental security of our systems
- ISO 27001 Certified co-location centers
- 24x7 guarded
- Access to systems is limited to SAI Global hosting services personnel

## DATA STORAGE, BACKUP AND RECOVERY

SAI Global has implemented secured onsite and offsite backups to ensure a seamless experience for your critical risk management systems.

- Customer data is stored on an enterprise storage array providing maximum performance, protection and data integrity, and in APAC & Americas, storage encryption.
- Offsite disaster recovery replication in real-time, with RPO of one hour and RTO of four hours.
- Daily data backups are replicated over our private network to the DR site under SAI Global control at all times.
- We keep 28 days of full database back-ups onsite, and 12 months offsite.

## NETWORK SECURITY

SAI Global segments sensitive production servers and data behind a state of the art firewall.

- SAI Global uses restrictive firewall policies for perimeter defense and a 3 tiered architecture which provides multiple segregated security zones for maximum data protection, from external, or internal attacks.
- We monitor production systems and network components, including internal system performance metrics, database health.
- We commission trusted third parties to undertake regular external network and web application penetration tests.
- We undertake weekly internal vulnerability scans of all systems and infrastructure, with annual network and Web application pen tests.

## APPLICATION SECURITY AND AUTHENTICATION

SAI provides extensive self-service control to each of our customers and has applied strong security measures by default.

- Passwords are encrypted using SHA 256 hashing algorithm. Data encryption at rest is defined per application and per customer requirements. When used, Encrypted Data will use AES256 bit as a minimum.
- The application is entirely rights and role-driven. Users only see what they have been given permission to see.
- The application supports Single Sign-On (SSO), which requires users to be authenticated via their identity provider using the SAML 2.0 or Shibboleth protocols.
- All data access occurs through the application via HTTPS (TLS 1.2). Direct access to the database is never afforded.
- If not using SSO, password attributes are configurable by each customer including password complexity, password history and password reuse, failed login attempt count and lockout time, and challenge questions.
- Application access can be limited to one or more ranges of IP addresses.

## INTEGRATIONS

SAI Global provides several methods of integration with third party applications using web services and data integration tools. Local applications can also be integrated with SAI Global's solutions. Third party integration consulting is available.





SAI GLOBAL