Security Statement

SignAgent SaaS Solutions Security Statement

Last Updated: February 5, 2018

1 SignAgent SaaS Production Environment

SignAgent employs a public cloud deployment model using both physical and virtualized resources for its software-as-a-service solutions (“SaaS Solutions”). All maintenance and configuration activities are conducted by SignAgent employees, primarily remotely from our corporate office.

SignAgent SaaS Solutions are multi-tenant and logical access controls using authentication and roles ensure the necessary separation between data from different clients. All infrastructure responsibilities rest with SignAgent, and clients are provided with functionality to manage their own users and roles at the application level.

SignAgent follows guidance from the ISO/IEC 27002:2013 standard as well as the OWASP Application Security Code of Conduct for Development Organizations.

1.1 Scalability

SignAgent distributed architecture for data collection, processing and reporting allows it to scale horizontally as the number of clients and volume of traffic increase. SignAgent uses multiple monitoring processes and tools to continuously track network resources, operating systems, applications and capacity. Systems are load balanced and scaled up when predetermined capacity thresholds are reached.

1.2 SaaS Management

SignAgent SaaS operations team (“SaaS Operations”) is responsible for all aspects of the SaaS Solutions production environment. SaaS Operations is set up separately and independently from the corporate network IT organization to ensure the necessary separation of duties. SaaS Operations’ professional depth enables SignAgent to provide SaaS services at the highest levels of efficiency.

2 Risk Management

SignAgent business continuity planning includes practices to assist management in identifying and managing risks that could affect the organization's ability to provide reliable services to its clients. These practices are used to identify significant risks for the organization, initiate the identification and/or implementation of appropriate risk mitigation measures, and assist management in monitoring risk and remediation activities.

SignAgent evaluates and manages risks related to its SaaS Solutions throughout their lifecycle, taking into considerations the consequences for our clients of loss of confidentiality or availability of the information we collect, process and store.

SignAgent maintains coverage to insure against major risks. Coverage is maintained at levels which SignAgent considers reasonable given the size and scope of its operations.

3 Security Policies & Organization of Information Security

3.1 Policies

SignAgent maintains a general Security Policy, updated annually, that explicitly addresses the confidentiality, integrity and availability of client data and information technology resources, and details employee's responsibilities and managements' role.

3.2 Information and Communication

SignAgent utilizes various methods of communication, such as email and instant messaging to update employees on current events and policies, and share information relevant to employees, such as industry news, training and development materials, employee resources, and other corporate policies.

3.3 Segregation of Duties

Only authorized personnel can administer systems or perform security management and operational functions. Authorization for and implementation of changes are segregated responsibilities wherever appropriate to the organization.

4 Human Resources Security

4.1 Employees

SignAgent policy prohibits employees from using confidential information (including Client Data) other than for legitimate business purposes, such as providing technical support.

4.2 Terms of Employment

SignAgent operates an onboarding process including at a minimum the following steps:

- Communication to the new employees of policies, code of conduct and behavioural standards.
- Employee signature of the employment agreement (which includes a confidentiality agreement) and SignAgent Security Policy.

5 Asset management

All data collected by SignAgent on behalf of its clients is the property of the respective clients and classified as highly confidential. Access to client data is restricted to legitimate business use only.

SignAgent generally performs no additional encryption on data collected and stored within the SignAgent SaaS production environment.

5.1 Client Data Location

All client data is processed and stored in the United States. Collected client data may transit temporarily through other centers in the United States, Europe, and Asia for optimal performance based on the visitor’s location and the regional option selected by the client.

5.2 Media Handling

SignAgent Security Policy prohibits copying client data on removable media device, including flash drives, hard drives, tapes or other media, other than for legitimate business purposes.

6 Access Control & Physical Security

6.1 User Access Management

Accounts on SignAgent SaaS production network, including for network administrators and database administrators, are mapped directly to employees using unique identifiers based on employee names.

6.2 User responsibilities

SignAgent Security Policy requires employees to notify corporate IT immediately if they believe that the security of their password has been compromised.

6.3 System and Application Access Control

Authentication and robust access controls ensure that all clients' confidential information is secured against unauthorized access. Users of SignAgent SaaS Solutions must be authenticated before they can access their data, and rights associated to their credentials control access to the logical structures containing their data.

Access to client data is limited to legitimate business need, including activities required to support clients' use of the SaaS Solutions. Employees may only access resources relevant to their work duties.

6.3.1 Data Access by Clients

Client end users are authorized only to see data from their account and may have additional privilege restrictions placed on their access to the account by their account administrator.

Client end users are identified with a username and password. They authenticate to the system over an HTTPS connection.

6.3.2 Access control to program source code

Write access to SignAgent SaaS production source code is limited to the engineering staff.

7 Physical and Environmental Security

SignAgent SaaS Solutions infrastructure is physically separated from SignAgent corporate facilities and uses a combination of colocation data center providers and Infrastructure-as-a-Service (IaaS) providers.

8 Supplier Relationships

SignAgent may use contractors for development and testing tasks. These individuals work under the direct supervision of SignAgent employees and may have access to client data where contractually permitted.

SignAgent doesn't give suppliers direct access to client data or network/equipment management responsibility. Colocation providers have access to the facility hosting the infrastructure, and may provide remote-hand service for hardware maintenance under SignAgent supervision, but they do not have direct access to client data or the SignAgent SaaS Solutions network environment.

SignAgent uses exclusively world renown third party suppliers with stellar background, such as Amazon (for cloud infrastructure).

SignAgent reviews ISO certification of its infrastructure providers to confirm their adherence to industry standard security and operational requirements.

9 Compliance

SignAgent complies with statutory and regulatory requirements, and uses reasonable efforts to comply with applicable industry standards.