Security, Privacy and Architecture Documentation

Corporate Trust Commitment
Area 1 Security is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Area 1 Security’s Master Subscription Agreement.

Services Covered
This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to, Area 1 Security Horizon.

Architecture and Data Segregation
The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Customer IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the “Infrastructure and Sub-processors” documentation available here.

Area 1 Security Horizon runs on .Public Cloud Infrastructure. This means the underlying physical infrastructure on which your Customer Data is stored will be with a public cloud provider for what is commonly referred to as Infrastructure as a Service, or Software as a Service, and the Covered Services will run on top of the public cloud provider.

Control of Processing
Area 1 Security has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Area 1 Security and its sub-processors. In particular, Area 1 Security and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Area 1 Security and its sub-processors are subject to regular audits. The “Infrastructure and Sub-processors” documentation
describes the sub-processors and certain other entities material to Area 1 Security’s provision of the Covered Services.

## Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use. Please see additional information on such controls in the Area 1 Security Horizon Security Guide.

Area 1 Security uses the following cloud providers to host our infrastructure. Each provider has an extensive set of security controls and certifications.

**Amazon Web Services (AWS):** For further information about security provided by AWS is available from the [AWS Security website](https://aws.amazon.com/security/), including AWS’s overview of security processes.

**Google Compute Platform (GCP):** For further information about security provided by GCP is available from the [GCP Security website](https://cloud.google.com/security), including GCP’s compliance offerings, security offerings, and privacy offerings.

**Microsoft Azure (Azure):** For further information about security provided by Azure is available from the [Microsoft Trust website](https://azure.microsoft.com/en-us/security/), including GCP’s compliance offerings, security offerings, and privacy offerings.

## Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, Area 1 Security can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Certain administrative changes to the Covered Services (such as password changes and adding custom fields) are tracked in an area known as the “Audit API” and are available for viewing by a customer’s system administrator. Customers may download and store this data locally.
- Area 1 Security personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.
Intrusion Detection

Area 1 Security, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Area 1 Security may analyze data collected by users' web browsers for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Area 1 Security maintains security incident management policies and procedures. Area 1 Security notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Area 1 Security or its agents of which Area 1 Security becomes aware to the extent permitted by law.

Area 1 Security publishes system status information on the Area 1 Security Status website as well as within the service portal. Area 1 Security provides its services adhering to enterprise level assurances, as outlined in the SLA document. Customers can choose to subscribe to service and incident notifications through their preferred method between emails or SMS texts. Area 1 Security typically notifies customers of significant system incidents using the notification of our status system. Root Cause Analysis (RCA) documents are published after the incident for customers to review the cause and corrective actions taken to resolve and avoid similar incidents.

User Authentication

Access to Covered Services requires authentication via one of the supported mechanisms as described in the Area 1 Security Guide, including user ID/password and 2FA, SAML-based Federation, or delegated authentication as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state. Session states timeout 4 hours after a logon occurs. In Mid 2020, this parameter will be customer configurable on-demand.

Physical Security

Production data centers used to provide the Covered Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems.
systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and backed up to localized data stores. Backups are verified for integrity and stored in the same data centers as their instance. The foregoing replication and backups may not be available to the extent the customer may request the deletion of Customer Data submitted to such services without any possibility of recovery.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Area 1 Security production facilities at the primary data centers were to be rendered unavailable.

Area 1 Security has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation.

The Covered Services’ disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service (recovery time objective) within 12 hours after Area 1 Security’s declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments.

Service levels, assurances and recoveries are governed by Enterprise SLAs as referred to in the SLA document. Area 1 is obligated at all times to adhere to those SLAs, and in the rare event of a temporary service failure, it is Area 1’s responsibility to recover systems within a specific time window such that the SLA is complied with. Our overall RPO and RTO for the service is 0-4 hours.
Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

Analytics

Area 1 Security may track and analyze the usage of the Covered Services for purposes of security and helping Salesforce improve both the Covered Services and the user experience in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Area 1 Security may share anonymous usage data with Area 1 Security’s service providers for the purpose of helping Area 1 Security in such tracking, analysis and improvements. Additionally, Area 1 Security may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Interoperation with Other Services

The Covered Services may interoperate or integrate with other services provided by Area 1 Security or third parties. Security, Privacy and Architecture documentation for services provided by Area 1 Security is available from support@area1security.com. Area 1 Security also provides a variety of platforms and features that allow Area 1 Security users to learn about Area 1 Security products, participate in communities, connect third party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Area 1 Security may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, Area 1 Security may contact users to provide transactional information about the Covered Services; for instance, through the Adoption Manager program or through system-generated messages, such as notifications. Area 1 Security offers customers and users the ability to deactivate or opt out of receiving such messages.