COMPUTE SOFTWARE INFORMATION SECURITY FRAMEWORK

Compute Software applies reasonable and appropriate administrative, technical, physical, organizational, and operational safeguards and processes to protect Customer Data against accidental and unlawful destruction, alteration, and unauthorized or improper disclosure or access. Compute Software has based its security framework on ISO 27001 standards, which is an international practice standard for information security management. Compute Software has certified to the EU-U.S. Privacy Shield Framework regarding the processing of data originating within the European Union and transferred to our servers in the United States. Compute Software will comply with the following safeguards in connection with the Services.

Personnel Background Checks & Training

All Compute Software personnel go through a background screening process prior to start. Further, all Compute Software personnel go through security and privacy awareness training on start, as well as annually thereafter. They are required to sign non-disclosure agreements and sign off that they have read and agree to adhere to Compute Software's security policies which include security and privacy safeguards of Customer Data.

Network Security

Compute Software takes commercially reasonable measures in compliance with best industry practices to prevent disclosure or dissemination of Customer Data to any person not having a need to know of or access to such information. Compute Software maintains access controls and policies to manage access from each network connection including the use of firewalls or functionally equivalent technology. Least privilege based authentication and authorization controls are maintained and periodically reviewed to ensure that access can only be granted to Compute Software personnel whose function and/or duties justifies such access. Some of the additional systems in place to maintain a strong and robust security infrastructure include IDS, centralized log management and alerting. All Service traffic routes through limited public interfaces via Compute Software's demilitarized zone (DMZ), which is firewalled. All inbound traffic is routed and filtered to more secure network segments.

Intrusion Detection, Logging & Monitoring

Compute Software creates, protects and retains information system log records to the extent needed to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity, including successful and unsuccessful account logon events, account management events, security events, object access, policy change, administrator account creation/deletion and other administrator activity, data deletions, data access and changes, IDS/IPS logs, firewall logs, and permission changes. Compute Software monitors for and conducts regular reviews for indications of inappropriate or unusual activity, and Compute Software protects log records from unauthorized access, unauthorized release, loss, modification, falsification, and deletion.

Physical Security

Compute Software's data is stored on Amazon Web Services (AWS), Auth0, HubSpot, InfluxData (InfluxDB Cloud), SendGrid, Mixpanel, and Google Workspace.

- AWS is ISO27001 certified, PCI DSS Level 1 compliant, and SAS70 Type II. In AWS based environments, Compute Software deploys, customizes and secures a Virtual Private Cloud (VPC) reducing the surface area of running services to only what is required to provide the Services. Learn more about AWS security.
- Auth0 is ISO27001 certified, PCI DSS Level compliant and SOC2 Type 2 certified. Learn more about Auth0 security.
- HubSpot is SOC2 Type 1 certified. Learn more about HubSpot security.
- InfluxData is SOC2 Type 1 certified. Learn more about InfluxData security.
- SendGrid is SOC2 Type 2 certified. Learn more about SendGrid security.
- Mixpanel is SOC2 Type 2 certified. Learn more about Mixpanel security.
- Google Workspace is ISO27001 certified, and SOC2 and SOC3 certified. Learn more about Google security.

Cloud Service Account Access

Amazon Web Services

Compute Software uses roles for cross-account access which is the current best practice for granting access to resources in one account (yours) to a trusted principal in a different account (Compute Software). Compute Software does not require an IAM User nor does it require you to share Access Keys. Roles created to grant Compute Software access to your account follow a specific policy that can easily be revoked by you at any time. Compute Software always uses an external ID when assuming the cross-account role, according to the AWS best practices to avoid the "confused deputy" problem.

Microsoft Azure

Cost Data

Compute Software uses Enterprise Agreement (EA) API Access Keys to collect cost data from Microsoft Azure. This is Azure's best practice for obtaining cost data. API Keys are uploaded to Compute Software over an encrypted connection and can be revoked and regenerated by you at any time. The Azure Platform requires these API keys to be rotated every 6 months.

Utilization Data

Compute Software uses Azure's Enterprise Applications with federated role-based access to collect infrastructure utilization metrics from your Azure environment. You trust Compute Software's enterprise application and provide it read-only access to this metric data.

Google Cloud Platform

Compute Software uses service accounts for access. Service accounts created to grant Compute Software access to your account follow the principle of least privilege. Permissions can be revoked by you at any time.

Application Security

Compute Software utilizes a multi-tier architecture which segregates the web service and application layers from the database layer, with each layer firewalled and limited from other layers via access control lists or security groups. Within the most secure segments, all Customer Data is encrypted at rest and logically isolated from other Compute Software customers.

Internet traffic in connection with our Services is encrypted with HTTPS/TLS with AES256 bit encryption and related application authentication is performed over this connection; weaker encryption ciphers are not supported. User identification and password transfer is at login only, after which a cryptographically strong random token is used. Account passwords are stored in the database using a strong, one-way cryptographic salted hash. Alternatively, integration with identity management platforms for authentication and authorization is supported and encouraged using standard protocols such as SAML (Single-Sign-On).

Anti-Virus/Anti-Malware
Compute Software uses virus and malicious code detection and protection products consistent with industry standards on all workstations and servers used to provide Services to Customer which are updated daily.

Vulnerability Management
Compute Software conducts regular internal and external scans for network and system vulnerabilities of applications that contain Customer Data. Compute Software uses a risk-based approach to determine the timing for remediation of the vulnerabilities, and remediates or mitigates critical or high risk vulnerabilities.

Compute Software uses automated software to conduct network and application vulnerability testing of Compute Software's information technology infrastructure (including servers, network devices, applications and databases) on a regular basis. The scope includes OWASP Top 10 among other potential threat vectors. All findings are assessed and remediated commensurate to the finding's severity level. Compute Software shall make these reports available to Customer upon request, which test reports shall be Compute Software's confidential information pursuant to the confidentiality terms between the parties. The report shall contain any findings, Compute Software's remediation, and any risk acceptance. If the report identifies any deficiencies, Compute Software will provide Customer with Compute Software's plan of action to correct the deficiencies, which at a minimum will include: (i) details of actions to be taken by Service Provider and/or its subcontractors to correct the deficiencies, and (ii) target dates for successful correction of the deficiencies. Compute Software will provide the action plan within thirty (30) days of request.

Security Notifications
In the event Compute Software has actual, confirmed knowledge of any unauthorized or reasonably likely unauthorized access to or acquisition of Customer Data in a manner that renders misuse of the information reasonably possible, Compute Software will, subject to an any applicable laws, (a) promptly, without undue delay, notify affected Customers as required by applicable law and (b) take commercially reasonable measures to address the issue in a timely manner. On a timely basis, Compute Software shall provide all relevant information available to Compute Software to Customer in connection with such security incident, including the following: (i) a description of the nature of the incident; (ii) the name and contact information of a point of contact where additional information may be obtained; and (iii) a description of the measures taken or proposed to be taken to remedy the

incident, including measures to mitigate negative effects. Compute Software will provide Customer with periodic updates about all developments in connection with the foregoing.

Third Party Security Assessment
Compute Software uses third party service providers to provide a discrete service to Compute Software for the purposes of enabling a portion of the Services.

Prior to the use of any information system introduced into the Compute Software platform and production environments, Compute Software ensures that new systems and technologies are appropriately vetted and approved for use. The vetting process may include researching vendor histories to best determine their security posture and potentially any issues with vulnerabilities and/or breaches of security.

Secure Application Development
Security is pervasive throughout the software development life cycle (SDLC). Compute Software's development and quality assurance engineering teams are required to attend secure software development training annually, focused on secure coding and OWASP Top 10 vulnerabilities. All code check-ins require a code review by a qualified engineer, and code is also tested using static code analysis on a regular basis. During the quality assurance portion of the SDLC, all components are tested using both automated and manual means. Web application vulnerability scans are performed against all applications and the resulting findings are remediated.

Data Destruction
Compute Software develops, implements and maintains appropriate measures designed to properly destroy or otherwise sanitize Customer Data prior to disposal, including release of technology infrastructure and assets used to process Customer Data out of organizational control, or release of such systems for reuse.

Audit and Assessment
Once per year upon reasonable prior written notice, Customer and its authorized representatives (including regulators and independent auditors) may, during normal business hours and subject to confidentiality obligations herein and reasonable access restrictions, conduct audits of Compute Software’s records and facilities to verify Compute Software’s compliance with the terms of this Framework Agreement. Compute Software will make personnel available as reasonably necessary to answer questions or otherwise assist Compute Software in connection with the same. Any such audit rights shall not permit Customer or its authorized representatives to require (i) physical or network access to any of Compute Software’s systems, (ii) access to materials, data, or information that is (a) unrelated to the Services provided to Customer by Compute Software; (b) that by its disclosure would cause Compute Software or any of its affiliates to be in breach of any confidentiality obligation to any party; (c) such disclosure would be a violation by Compute Software of applicable laws; or (d) if such disclosure would hinder law enforcement’s investigation into a security event, (iii) any action or disclosure that could reasonably result in a compromise to the efficacy of the information security program or security certifications of Compute Software, or (iv) any results of security vulnerability assessments identifying specific security vulnerabilities. Notwithstanding the foregoing, in lieu of an audit

right relating to compliance by Compute Software of its security obligations pursuant to this Framework Agreement, Compute Software may provide written responses to questions regarding its privacy and information security practices that apply to Customer Data.

Access Control

Compute Software employs the principle of least privilege in all cases, ensuring that only those who are responsible for, or working directly with, a resource have access to that resource at any given point in time. The highest due diligence and care is placed on systems hosting customers (and the associated Customer Data). Several controls are in place to prevent unauthorized access to Customer Data.

Encryption & Key Management

Compute Software uses industry-standard encryption and key management systems to protect Customer Data while in storage and during transmission between Customer's network and Compute Software's SaaS solution, including through Transport Layer Encryption (TLS 1.2 or above) leveraging at least 2048-bit RSA server certificates and 256 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 at least AES-256 encryption.

Continuous Evaluation

To help ensure security, integrity and availability for our Customers, Compute Software performs periodic, continuous evaluation of its policies and procedures directly.
Compute Softwares information security practices will evolve over time to keep pace with appropriate industry standards and as such this overview is subject to revision.