

KALIBRATE INFORMATION SECURITY PRACTICES

V1.1

1. DISCLAIMER

The information contained in this document represents the current view of Kalibrate as of the date of its publication. This document and its contents are subject to modification by Kalibrate in its absolute discretion. Kalibrate does not guarantee that the information contained in this document will be error-free or kept up to date after its publication. TO THE EXTENT PERMITTED BY APPLICABLE LAW, KALIBRATE MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, ABOUT THE INFORMATION CONTAINED IN THIS DOCUMENT.

2. INFORMATION SECURITY PROGRAM

Kalibrate maintains an Information Security Program which includes appropriate physical, technical and administrative safeguards sufficient to protect any client data or confidential information ("Client Data") from unauthorized or unlawful destruction, loss, alteration, disclosure or access. Further, Kalibrate maintains various policies including Information Security Policy, Acceptable Use Policy, Incident Management Policy etc., with objectives and targets set and monitored to achieve continual improvement of Information Security Program.

3. TECHNICAL CONTROLS

Kalibrate maintains, where appropriate, certain technical controls to ensure the security of Client Data. However, the internet is an open system and Kalibrate does not warrant or guarantee that third parties cannot or will not intercept or modify Client Data outside of the application.

4. DATA BACK UP

Client Data will be backed up on a frequency appropriate to ensure the Recovery-Point-Objective (RPO) as detailed herein. Client Data backups will be stored within the same geographic area as the rest of the Client Data, so as to preserve data residency and compliance boundaries. Kalibrate may from time to time test its backup systems and may use copies of Client Data as part of these tests. In the event of a disaster, (i) Kalibrate provides a Recovery Time Objective (RTO) of 24 hours from the point of a disaster being declared and the recovery plan subsequently being invoked; (ii) RPO will be a maximum of fifteen (15) minutes.

5. MONITORING

Kalibrate will use reasonable endeavours to monitor the cloud solution. This will include automated alerts on the availability, welfare, performance and security of the components comprising the cloud solution.

6. INCIDENT MANAGEMENT

Kalibrate maintains a Business Continuity / Disaster Recovery Plan to ensure business operations' continuation during an emergency, natural disaster, or cybersecurity threat. Kalibrate will test such plan periodically at its discretion to ensure the effectiveness of the plan. If any breach of Kalibrate's Information Security Program leads to the accidental or unlawful or unauthorized destruction, loss, alteration, disclosure of, or access to any client's data or confidential information (each a "Data Breach Incident"), Kalibrate will make reasonable efforts to investigate such Data Breach Incident, and subject to verification, promptly notify the affected client(s). The notice will summarize the nature and scope of the Data Breach Incident and the corrective action already taken or planned by Kalibrate. Kalibrate will take all reasonable actions to mitigate the Data Breach Incident. Kalibrate will reasonably cooperate with affected client(s) in the investigation and remediation of the Data Breach Incident.

7. CERTIFICATIONS

Kalibrate certifies annually for SOCI and SOCII Type 2 compliance, covering all 5 trust service principles of Security, Availability,

Processing Integrity, Confidentiality and Privacy, encompassing the following scope (2022/2023):

- Kalibrate Software as a Service (SaaS) product suite(s)
 - Kalibrate Pricing (SaaS)
 - including DATA, Ingestion, ConnectV2 and Science API's
 - Kalibrate Planning (SaaS)
- KLI Software as a Service (SaaS) product suite(s)
 - TAS Online, TAS Mobile, TAS Management Studio, TAS API
- Intalytics Software as a Service (SaaS) product suite(s)
 - SiteIntel and SiteIntel API(s)
- Trailblazer Software as a Service (SaaS) product suite(s)
- Single Site Analysis
- TrafficMetrix
- KENT Charting

8. HOSTING PARTNER SECURITY PRACTICES

Kalibrate utilises services from Microsoft Corporation and AWS to host its solutions. Microsoft and AWS follows ISO27001 and SOC 2 Type 2 certifications and other industry standard security practices. More information about Microsoft's and AWS's security compliance can be found in the following links.

<https://learn.microsoft.com/en-us/azure/compliance/>

<https://aws.amazon.com/compliance/services-in-scope/>

9. INFOSEC POINT OF CONTACT

Kalibrate's primary information security point of contact is:

Head of Information Security
Kalibrate Technologies
Suite 213
No.2 Circle Square
1 Symphony Park
Manchester, England, M1 7FS
United Kingdom
Phone: +44 161 609 4000

infosec@kalibrate.com