GroupMap Technology Pty Ltd
SOC 3 for Service Organizations Report

1 March 2023 to February 2024

assurancelab

CONTENTS

SECTION I –

ASSERTION OF GROUPMAP TECHNOLOGY PTY LTD MANAGEMENT

ASSERTION OF GROUPMAP TECHNOLOGY PTY LTD MANAGEMENT

20 May 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within GroupMap Technology Pty Ltd's ('GroupMap Technology') TeamRetro Software as a Service System (the 'System') throughout the period 1 March 2023 to 29 February 2024 to provide reasonable assurance that Groupmap Technology's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy ('Agreed Criteria') set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in 'Groupmap Technology's Description of its System' (the 'Description') and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period 1 March 2023 to 29 February 2024 to provide reasonable assurance that Groupmap Technology's service commitments and system requirements were achieved based on the Agreed Criteria. Groupmap Technology's objectives for the System in applying the Agreed Criteria are embodied in its service commitments and system requirements relevant to the Agreed Criteria. The principal service commitments and system requirements related to the Agreed Criteria are presented in 'Groupmap Technology's Description of its System.'

GroupMap Technology uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap Technology's controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of GroupMap Technology's controls. The Description does not disclose the actual controls at the subservice organization.

The Description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap Technology's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of GroupMap Technology's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the period 1 March 2023 to 29 February 2024 to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria.

Jeremy Lu
Chief Executive Officer
GroupMap Technology Pty Ltd

SECTION II –
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: GroupMap Technology Pty Ltd

Scope

We have examined GroupMap Technology Pty Ltd's ('GroupMap Technology') accompanying description of its TeamRetro Software as a Service System (the 'Description') which has been prepared for the purposes of the independent assurance report.

GroupMap Technology prepared the Description based on the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about the GroupMap Technology's TeamRetro Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with GroupMap Technology's System. This includes the controls that GroupMap Technology has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

GroupMap Technology uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organization controls have been reviewed by GroupMap Technology management. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description includes complementary user entity controls that are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap Technology's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of GroupMap Technology's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

Service Organization's Responsibilities

GroupMap Technology is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved. GroupMap Technology has provided the accompanying assertion titled "Assertion of GroupMap Technology Pty Ltd Management" (the 'Assertion') about the Description and the suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. GroupMap Technology is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable Agreed Criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the GroupMap Technology's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of controls stated in the Description based on our examination. Our examination was conducted in accordance with AT-C 105 and AT-C 205 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

- The Description is presented in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed.
- The controls stated in the Description were operating effectively throughout the period to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the Description of GroupMap Technology's System and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the System and GroupMap Technology's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that GroupMap Technology achieved its service commitments and system requirements based on Agreed Criteria.

- Testing the operating effectiveness of controls stated in the Description to provide reasonable assurance that GroupMap Technology achieved its service commitments and system requirements based on the Agreed Criteria.
- Evaluating the overall presentation of the Description.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the System that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within GroupMap Technology's System were effective throughout the period 1 March 2023 to 29 February 2024, to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria is fairly stated, in all material respects.

AssuranceLab CPAs LLC

AssuranceLab CPAs LLC
Austin, Texas
United States
20 May 2024

SECTION III –
GROUPMAP TECHNOLOGY PTY LTD'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

GroupMap Technology Pty Ltd ('GroupMap Technology') was founded in September 2012 to develop Software as a Service meeting and group decision-making tools.

GroupMap is a distributed company, with primary headquarters based in Perth, Australia.

Industries served include information technology and communications, financial services, telecommunications, pharmaceutical, manufacturing, consumer goods, gaming and entertainment, healthcare, retail, education, and government.

Description of Services Provided

GroupMap Technology's product, TeamRetro, is designed to facilitate efficient retrospective and health check sessions for agile teams, suitable for both in-person and remote settings. As a cornerstone of Agile and Scrum frameworks, retrospectives enable teams to review their latest work cycle, identify successes and areas for improvement, and devise practical strategies to boost future outcomes.

The TeamRetro product enables processing of:

- Agile retrospective meetings
    - Capturing ideas
    - Capturing reactions
    - Grouping related / similar ideas
    - Capturing user reactions to ideas
    - Capturing user votes on ideas worth discussing forward
    - Capturing proposed / accepted action items
    - Capturing proposed / accepted team agreements
    - Publishing retrospective summaries to external systems (such as Confluence, Slack)
- Agile health check meetings
    - Capturing ratings along user-defined health dimensions
    - Capturing response comments related to health dimensions
    - Capturing discussion along health dimensions
    - Capturing proposed / accepted action items
    - Capturing proposed / accepted team agreements
    - Publishing health check summaries to external systems (such as Confluence)
- Team action items
    - Capturing proposed / accepted action items
    - Capturing action status
    - Publishing actions to external task management systems (such as Jira, Trello, Azure DevOps)
- Team agreements
    - Capturing proposed / accepted team agreements
- Reporting & Insights
    - Team health insights and reports

  - Team activity insights and reports
  - User activity insights and reports
  - Action insights and reports
  - Exports in multiple data formats (such as XLS, CSV)
- SAML for SSO
- SCIM for team provisioning
- API access

Retrospectives

Retrospective templates can be used to capture ideas, comments, and reactions from participants against a series of retrospective trigger prompts such as *What went well*?, *What didn't go well?* etc. Ideas are then grouped and voted on to prioritize for deeper discussion. Each group is then discussed, in turn enabling additional comments. Reactions can be added by participants, and new action items or team agreements can be proposed or added against these groups. Finally, action items and team agreements are reviewed, assigned, and then shared with meeting participants.

Health Checks

Health check templates can be used to capture participant ratings and comments along key health dimensions such as *Codebase Complexity, Communication, Team Work* etc. Health dimensions are then sorted based on aggregate rating to prioritize for deeper discussion. Each dimension is then discussed in turn where participants can add further comments or propose or add new action items or team agreements. Finally action items and team agreements are reviewed, assigned, and then shared with meeting participants.

Both retrospective and health check activities can be run synchronously (with all participants online at the same time) or asynchronously (with each participant contributing at their leisure). Both activities can be run fully anonymously, partially anonymously, or named. Additional optional icebreaker questions, check-in questions and check-out questions are supported to further engage the team and gather additional feedback.

Principal Service Commitments and System Requirements

GroupMap Technology has established processes, policies, and procedures to meet its objectives related to its TeamRetro Software as a Service System (the 'System'). Those objectives are based on the purpose, vision, and values of GroupMap Technology as well as commitments that GroupMap Technology makes to user entities, the requirements of laws and regulations that apply to GroupMap Technology's activities, and the operational requirements that GroupMap Technology has established.

Security commitments to user entities are documented and communicated in data processing agreements, enterprise agreements and other customer agreements, as well as in public descriptions of the System. Security commitments are standardized and include security principles within the fundamental designs of the System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

GroupMap Technology establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in GroupMap Technology's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the System is designed and developed, how the System is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required for the operation and development of the TeamRetro product.

Components of the System

Infrastructure

GroupMap Technology's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of Amazon Web Services ('AWS').

System	Type	Description
Amazon Web Services (AWS)	Managed application servers (AWS ECS)	Server infrastructure for business logic and database binding and mapping to logic.
	Managed Postgres databases (AWS Aurora Postgres)	Storage of dynamic customer data.
	Managed Backups (AWS Backup)	Backups of customer data.
	Managed Redis databases (AWS Elasticache)	User session management, rate limiting and caching.
	Content delivery network (AWS CloudFront)	Low-latency, global delivery of static content.
	Cloud object storage (AWS S3)	Storage of static application and customer assets.
	Web application firewall (AWS WAF)	Application security and web application firewall.
	HTTP/S load balancing (AWS ELB)	Automatically distributes incoming application traffic across multiple targets.

System	Type	Description
	Managed Denial-of-service protections (AWS Shield)	Managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.
	Managed certificates (AWS Certificate Manager)	A service to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services.
	Managed encryption keys (AWS Key Management Service)	Centralized control over the cryptographic keys used to protect data.
	Networking infrastructure / logging infrastructure (AWS VPC, AWS Route53, AWS Application Load Balancer, AWS Systems Manager, AWS ECR, AWS CloudWatch, AWS CloudTrail), AWS SSO, AWS VPN	Core networking infrastructure, operational monitoring, and alerts.
DataDog	Infrastructure dashboards	Operational insights and alerts.
BetterStack	Logging (Better Logs)	Operational insights and alerts.
	Monitoring (Better Uptime)	Operational insights and alerts.
Rollbar	Error logging	Error logging.
MessageBird	Scalable WebSocket broadcasting (Pusher Channels)	Real-time WebSocket data synchronization.
Twilio	Email delivery (SendGrid)	Transactional emails.
PayPal	Payment Gateway (Braintree)	Online subscription payments.

Software

Primary software is used to support GroupMap Technology's System.

Software	Purpose
TeamRetro	The Software as a Service product provided to GroupMap Technology customers.
Bitdefender	Anti-virus software used to protect endpoint devices from malware.
FeatureOS	Product roadmap, customer feedback.
GitHub	Source code repository used to manage the software code and version control.
GitHub Actions	Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment.
Google Workspace	Google's suite of enterprise productivity, collaboration, and communication tools. Authentication software used to identify and authenticate users for access control to the systems.
1Password	Enterprise password manager used to store authentication secrets and strengthen password security.
Hexanode MDM	Mobile device management software used to track and manage security policies on endpoint devices.
Ninjio	Security awareness training program.
Codacy, Intruder.io	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
Linear	Team task management, also used to log events and requirements to support the internal controls.
Xero	Human resources information system used to manage employee processes like onboarding, offboarding and performance.
OneTrust	Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance. OneTrust was utilized from 19 August 2021 to 31 October 2023.

People

GroupMap Technology has 10 people that are organized into the following functional areas:

Area	Purpose
Corporate	Including Executives, Finance, Talent, and Human Resources.

Customer Experience	Including Customer Support, Customer Success, Customer Delivery and CX Operations teams. They provide day to day support to customers, whether dealing with issues from existing customers, to onboarding new customers, as well as how the company can uplift the overall customer experience.
Product Development	Including product management, UX design, as well as analysis, development and quality activities focusing on development and verification of the product.
Operations	Including infrastructure, development and quality activities focus on maintenance, security and reliability of the product, platform, and infrastructure.
Sales	Sales is driven by growth and its focus is on retaining existing clients and maximising advocacy in addition to growing existing customers and new customer acquisition.
Marketing	Provides company wide, consistent branding, positioning and drives programs to deliver sustainable growth.

Data

Data, as defined by GroupMap Technology, constitutes the following:

- User emails, names, avatars, and password hashes
- User activity: user activity within the software
- User content, including:
    - Retrospective data (ideas, reactions, groups, votes, comments, reactions, and survey responses)
    - Health check data (ratings, comments, and survey responses)
    - Team action items
    - Team agreements
    - Custom retrospective templates
    - Custom health check templates
    - SCIM groups and users
    - User requests
    - Reports
- Logs
    - Activity logs
    - Admin logs
    - API logs
    - Error logs
    - Integration logs
    - System logs
- Supporting data
    - Quotes
    - Invoices
    - Contracts

- Payment history
- Customer queries, tickets, and feature suggestions

Privacy Commitments

GroupMap Technology is a Data Processor. GroupMap Technology collects and processes personal data as part of the System at the direction of the Data Controllers who are GroupMap Technology's customers who use the System. The Data Subjects, whose personal information is collected, are the Data Controllers' employees (and other invited team members and guests).

Personally identifiable information collected from Data Subjects includes email address, full name, and internet protocol (IP) address. This information is collected through the online signup process, via invitation from an existing user, or via the optional SSO and SCIM integrations.

Data Subjects are presented with the governing TeamRetro Privacy Policy and TeamRetro Terms of Service for review while creating a new account. Any additional users invited to join the account are additionally presented the Privacy Policy and Terms of Service within the invitation emails sent by TeamRetro.

The full TeamRetro Privacy Policy is published on the TeamRetro website at https://www.teamretro.com/privacy and addresses how any personal information and intellectual property is collected, used, retained, disclosed, disposed, and anonymized.

The Privacy Policy also provides details of the assigned Privacy Officer, assigned EU Representative, and contact information including the primary privacy@teamretro.com email.

The following table describes the personal information collected and processed as part of the System of GroupMap Technology. Reports can be viewed in the TeamRetro application and are downloadable in electronic Adobe Acrobat (PDF), Microsoft Excel (XLSX) or comma-delimited (CSV) value file formats. The availability of these reports is limited based on user role.

The following table describes the personal information collected and processed as part of the System of GroupMap:

Private Data	Reporting
Retrospective data Ideas Reactions Groups Votes Comments Custom retrospective templates	Retrospective summary (PDF) Ideas report (CSV, XLSX) Ideas with comments report (CSV, XLSX) Actions report (CSV, XLSX) Retrospective activity report (CSV, XLSX) Team activity report (CSV, XLSX)
Health check data	Health check summary (PDF)

Private Data	Reporting
Ratings Comments Votes Custom health check templates	Latest health report (CSV, XLSX) Historical health report (CSV, XLSX) Actions report (CSV, XLSX) Health check activity report (CSV, XLSX) Team activity report (CSV, XLSX)
Team Team action items Individual team member action items Team agreements	Teams report (CSV, XLSX) Team activity report (CSV, XLSX) Individual action report (CSV, XLSX)
Users Usernames Email addresses Avatars Password hashes	Users report (CSV, XLSX)
Retrospective data Ideas Reactions Groups Votes Comments Custom retrospective templates	Retrospective summary (PDF) Ideas report (CSV, XLSX) Ideas with comments report (CSV, XLSX) Actions report (CSV, XLSX) Retrospective activity report (CSV, XLSX) Team activity report (CSV, XLSX)

GroupMap Technology is committed to attestation reporting for the SOC 2 Trust Services Criteria related to Privacy to demonstrate the governance, accountability, and alignment of its privacy commitments.

Processes, Policies and Procedures

Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with GroupMap Technology's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all GroupMap Technology's employees and can be referred to as needed.

Compliance Management Platform

GroupMap Technology uses task management software Linear and the Google Workspace platform to support the design, implementation, operation, monitoring, and documentation of the internal controls.

Physical Security

The critical infrastructure and data of the System are hosted by AWS. There are no trusted local office networks. As such, AWS is responsible for the key physical security controls that support the System.

Logical Access

GroupMap Technology's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfill job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Google Workspace authentication software is used for identity management and single-sign on. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are periodically reviewed and adjusted when no longer required. Additional information security policies and procedures require GroupMap Technology employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, periodic testing for and remediation of technical vulnerabilities, and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

GroupMap Technology employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Hexanode MDM mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

System Operations

Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

GroupMap Technology's critical infrastructure and data are hosted by AWS with multiple availability zones to provide failover capability in the event of an outage of one of the data centres. Redundancy and disaster recovery in continuity considerations is built into the system design of AWS to support GroupMap Technology's availability objectives. These are supported by system monitoring, incident management processes and defined recovery and continuity plans.

Change Control

GroupMap Technology operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the TeamRetro software to support GroupMap Technology's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub version control software is used for the code repository that tracks all changes to the TeamRetro software, including managing versions and roll-back capability in the event of a failed change release. A continuous integration / continuous deployment (CI/CD) pipeline is configured using Github Actions to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment. Changes to the infrastructure configurations and settings are managed as code, subject to the same process steps and checks prior to impacting the production environment.

Data Governance

GroupMap Technology uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of GroupMap Technology.

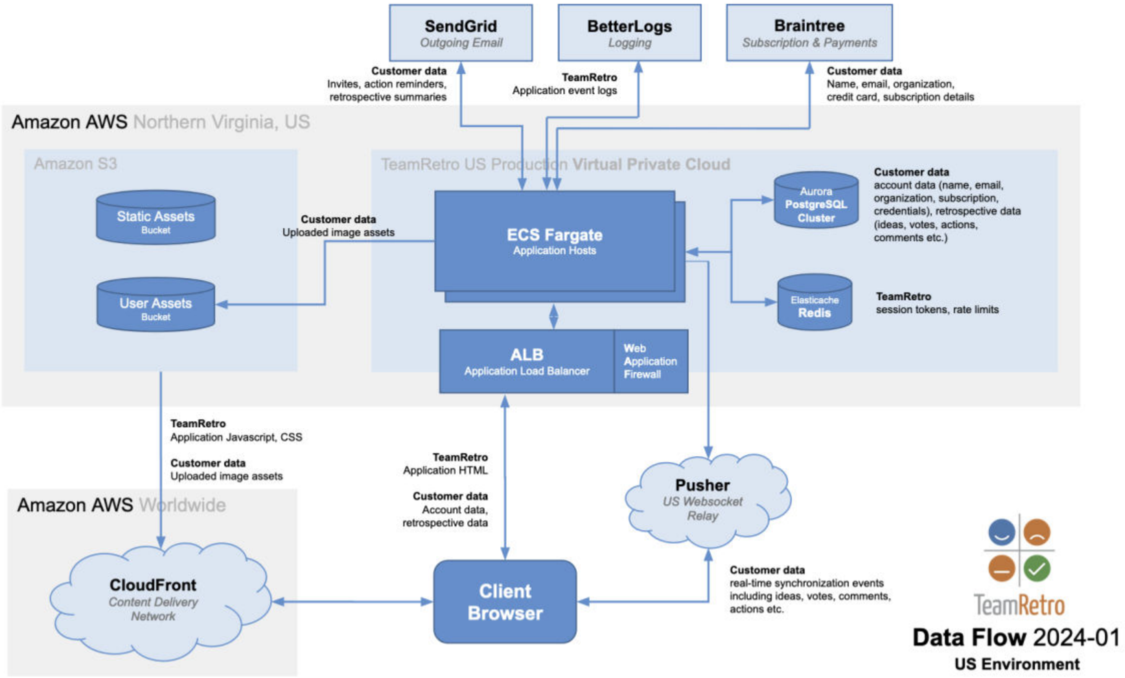
Established processes, policies, and procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Boundaries of the System

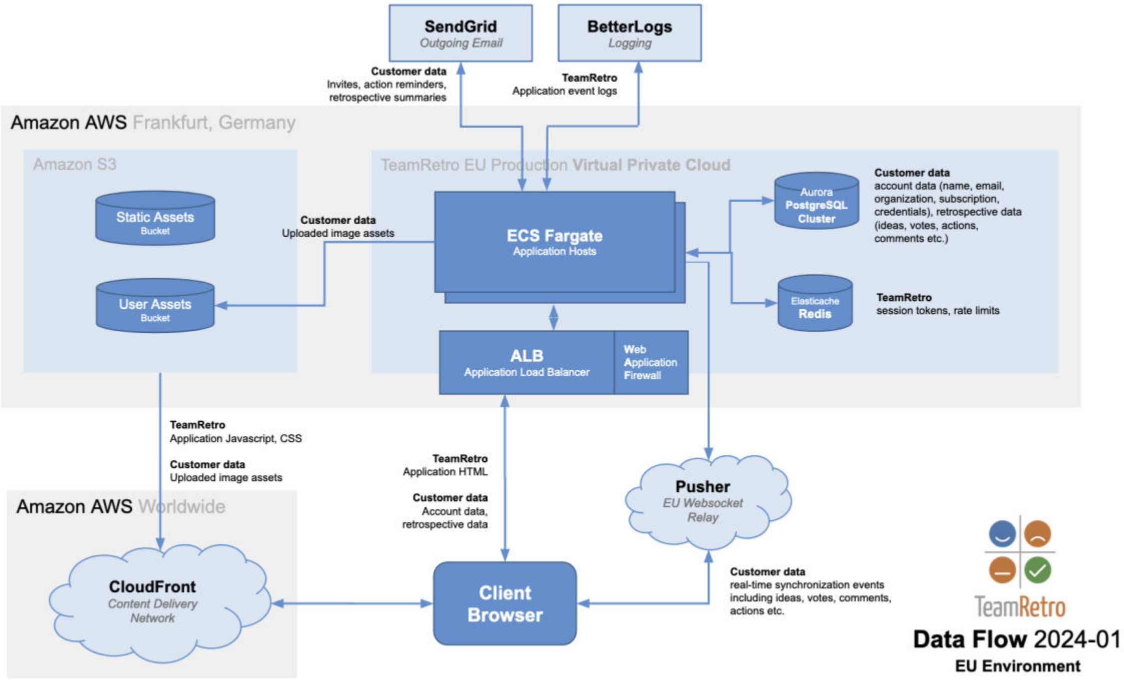
The scope of this report includes the GroupMap Technology System. This report does not include the cloud hosting services provided by AWS.

TeamRetro offers two hosting environments (US and EU). Customers who opt for the US environment have their data stored exclusively within AWS US-based data-centers (us-east-1), while customers who opt for EU environment have their data stored exclusively within AWS EU-based data-centers (eu-central-1).

TeamRetro US Environment



TeamRetro EU Environment



COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This report does not include the cloud hosting services provided by Amazon Web Services ('AWS').

Subservice Description of Services

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia.

Complementary Subservice Organization Controls

GroupMap Technology's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Agreed Criteria related to GroupMap Technology's services to be solely achieved by GroupMap Technology control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of GroupMap Technology.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – Amazon Web Services		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.1- CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.

Subservice Organization – Amazon Web Services		
Category	**Criteria**	**Control**
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply ('UPS') units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Critical AWS system components are replicated across multiple availability zones and backups are maintained.

GroupMap Technology management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, GroupMap Technology performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

COMPLEMENTARY USER ENTITY CONTROLS

GroupMap Technology's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Agreed Criteria related to GroupMap Technology's services to be solely achieved by GroupMap Technology control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GroupMap Technology's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Agreed Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

User entities are responsible for:

- Understanding and complying with the TeamRetro Terms of Service.
- Notifying GroupMap Technology of changes made to technical or administrative contact information.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Ensuring multi-factor authentication is applied by personnel, if required.
- Performing any required risk assessments and approvals when using pre-built integrations available with GroupMap Technology's services.
- Ensuring the supervision, management, and control of the use of GroupMap Technology's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize GroupMap Technology services for any critical reliance on these services.

Data controller responsibilities:

- User entities are responsible for obtaining consent from data subjects prior to the collection or processing of any personal data.
- User entities are responsible for having a privacy policy to notify data subjects of the requirements for consent, the choices available to data subjects and their rights in relation to the personal data.
- User entities are responsible for providing notice to their data subjects about its privacy practices to meet the user entity's objectives related to privacy.
- User entities are responsible for ensuring that personal information is collected consistent with the user entity's objectives related to privacy.
- User entities are responsible for communicating choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice.

- User entities are responsible for granting identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, providing physical or electronic copies of that information to data subjects to meet the user entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the user entity's objectives related to privacy.
- User entities are responsible for correcting, amending, or appending personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the user entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the user entity's objectives related to privacy.
- User entities are responsible for disclosing personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the user entity's objectives related to privacy.
- User entities are responsible for obtaining commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the user entity's objectives related to privacy.
- User entities are responsible for providing notification of breaches and incidents to affected data subjects, regulators, and others to meet the user entity's objectives related to privacy.
- User entities are responsible for providing data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the user entity's objectives related to privacy.
- User entities are responsible for providing data subjects with means of contacting the entity with inquiries, complaints, and disputes regarding personal information.

assurancelab