SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S DESCRIPTION OF ITS

TeamRetro Software as a Service System

Relevant to Trust Services Criteria for Security, Availability, Confidentiality and Privacy

For the period 1 March 2025 to 28 February 2026

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of GroupMap Technology Pty Ltd. (GroupMap Technology),

Scope

We have examined GroupMap Technology's accompanying assertion titled "Assertion of GroupMap Technology Management" (assertion) that the controls within GroupMap Technology's TeamRetro Software as a Service System (system) were effective throughout the period 1 March 2025 to 28 February 2026, 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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

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 about the effectiveness of controls within the system. When preparing its assertion, GroupMap is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve GroupMap Technology's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve GroupMap Technology's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

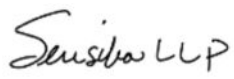
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria and also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness 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 TeamRetro Software as a Service System were effective throughout the period 1 March 2025 to 28 February 2026, to provide reasonable assurance that GroupMap Technology's services commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California

28 April 2026

2. Assertion of GroupMap Technology Management

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 throughout the period 1 March 2025 to 28 February 2026 to provide reasonable assurance that GroupMap Technology's service commitments and system requirements relevant to Security, Availability, Confidentiality and Privacy were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of GroupMap Technology's TeamRetro Software as a Service System" (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period 1 March 2025 to 28 February 2026 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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

GroupMap Technology's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

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 2025 to 28 February 2026, to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by GroupMap Technology Management

28 April 2026

3. Description of GroupMap Technology's TeamRetro Software as a Service System

Company Background

GroupMap Technology Pty Ltd ('GroupMap Technology') is an Australian-based, globally distributed software company founded in September 2012. Headquartered in Perth, Western Australia, the organization develops and delivers web-based Software-as-a-Service (SaaS) solutions designed to facilitate collaboration, inform decision-making, and enhance productivity. The company's products—most notably TeamRetro—are used by a wide range of organizations, from small startups to multinational enterprises. GroupMap Technology supports customers across Australia, New Zealand, Asia, the United States and Europe.

GroupMap Technology is committed to delivering secure, reliable, and privacy-focused collaboration services. TeamRetro is designed using modern cloud security principles, role-based access controls, encrypted communications, continuous monitoring, and formal operational processes to support customer trust and regulatory compliance.

The company serves a diverse range of industries, including:

- Information Technology
- Professional Services
- Financial Services
- Healthcare
- Government
- Defense
- Education
- Telecommunications
- Manufacturing
- Pharmaceutical
- Gaming and Entertainment
- Consumer Goods

The company employs a distributed workforce, leveraging modern cloud technologies and agile development practices to provide services to its global customer base. TeamRetro provides structured support for retrospectives, health checks, and other collaborative activities, enabling teams to maintain continuous improvement across diverse operational contexts.

TeamRetro

Services Provided

TeamRetro is GroupMap Technology's core web-based application, designed for agile teams to conduct structured retrospectives and team health checks. By facilitating structured collaboration, TeamRetro enables organizations to manage continuous improvement, track action items, and understand team sentiment and challenges.

Key Features and Functions

Retrospective Meetings:

- Prompts and Templates: Users can select or customize retrospective templates (e.g., "What Went Well?", "What Didn't Go Well?") to capture observations, ideas, and feedback.
- Idea Capture and Grouping: Participants add ideas anonymously or with attribution, then group and consolidate similar items for efficient discussion.
- Voting and Prioritization: Team members vote to identify top priorities for deeper analysis.
- Discussion and Reactions: As items are discussed, participants can add reactions, comments, and clarifications in real time.
- Action Items and Team Agreements: Based on discussions, new action items or team agreements can be proposed, documented, and assigned.
- Summary Publishing: Meeting outcomes can be exported or shared with third-party tools (e.g., Confluence, Slack, Notion) to keep stakeholders informed.

Health Check Meetings:

- Health Dimensions: Users rate and comment on key health factors (e.g., Codebase Complexity, Communication, Teamwork) using built-in or custom templates.
- Health Dimension Groups: Dimensions can be organized into logical groups, enabling structured assessment across related categories and supporting matrix-style response formats.
- Sorting and Analysis: Overall results are aggregated and sorted, highlighting the dimensions most in need of attention or improvement.
- Collaborative Discussion: Teams discuss each dimension, adding further comments, action items, or team agreements.
- Final Review: Action items and agreements are finalized, assigned, and shared with participants.

Estimation Meetings:

- Work Item Import: Teams import user stories, issues, or work items from integrated project management tools (e.g., Jira, Azure DevOps, Linear, GitHub) for estimation.
- Estimation Rounds: Participants estimate work items using configurable card decks (e.g., Fibonacci, T-shirt sizing, Powers of 2) in real-time planning poker sessions.

- Discussion and Re-estimation: After initial estimates are revealed, teams discuss outliers and can re-estimate to reach consensus.
- Point Synchronization: Agreed estimates can be synced back to the source project management tool automatically.
- Estimation Reports: Meeting outcomes are available as downloadable reports and within the cross-team insights dashboard.
- Retrospective, health check, and estimation features can be run synchronously (live) or asynchronously, and teams can choose whether to conduct these sessions anonymously or with full attribution.

AI Features:

- Retrospective Template Generation: Offers structured retrospective templates aligned with agile methodologies.
- Health Model Template Generation: Recommends health check dimensions based on industry best practices and team context.
- Icebreaker Question Generation: Suggests relevant, engaging prompts for quick team warm-ups.
- Retrospective Meeting Summarization: Auto-creates concise summaries of discussions, decisions, and action items.
- Health Check Meeting Summarization: Auto-creates concise summaries of health check discussions, highlighting key dimension ratings and trends.
- Health Dimension Summary: Generates narrative summaries of individual health dimensions, surfacing key themes from participant comments.
- Suggested Grouping: Clusters similar ideas to speed up organization and reduce manual work.
- Suggested Actions: Highlights potential tasks or improvements tied to meeting discussions.
- Suggested Group Titles: Provides clear, concise labels for grouped ideas or themes.
- Suggested Meeting Titles: Proposes memorable, context-specific names for sessions.

All AI synthesis features are powered by AWS Bedrock with Standard-tier Guardrails for content safety. AI processing adheres to GroupMap Technology's privacy commitments and does not expose personal data to unauthorized third parties.

Kudos and Mentions:

- Peer Recognition: Team members can give kudos and mentions to colleagues to recognize contributions.
- Badges and Counters: Recipients receive badges that are tracked and displayed within their profile.
- Notifications: Kudos recipients are notified via in-app and email notifications.
- Guest Participation: Guest participants can give kudos during sessions.

Team Action Items:

- Creation and Status Tracking: Users can propose, create, update, and track the status of action items arising from retrospectives or health checks, or estimation meetings.
- Integration: Actions can be published directly to third-party task management systems (e.g., Jira, Trello, Azure DevOps, Linear, Notion, Monday.com).

Team Agreements:

- Proposal and Acceptance: Teams can propose and finalize agreements for improved ways of working.
- Visibility: Agreements are visible in team dashboards for easy reference and follow-up.

Reporting and Analytics:

- Cross-Team Insights: High-level dashboards highlight usage trends, health metrics, and retrospective outcomes, and key sentiments across multiple teams.
- Activity and User Reports: Detailed logging and exports (PDF, CSV, XLSX, Markdown) help visualize participation and track progress on items over time.
- Search: Users can search across retrospective meetings to locate past sessions by keyword.
- Webhooks: Event-driven notifications can be delivered to external systems for real-time integration with customer workflows.
- API and SCIM: Offers programmatic access and provisioning capabilities for advanced integration with enterprise systems.

Principal Service Commitments and System Requirements

GroupMap Technology designs its processes and procedures related to its TeamRetro Software as a Service System (the ‘System’) to meet its objectives. Those objectives are based on the service commitments that GroupMap Technology makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that GroupMap Technology has established for the services. Security commitments to user entities are documented and communicated in service level agreements and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include security principles within the fundamental designs of the TeamRetro Software as a Service 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. The company is committed to delivering secure, high-performing services that meet the needs of diverse user

entities. The company's processes, procedures, and controls for TeamRetro are designed to fulfill the following obligations:

Service Commitments:

- Performance and Reliability: TeamRetro's architecture and operational procedures aim to provide high availability and rapid response times.
- Security and Privacy: TeamRetro's security posture is governed by robust administrative, technical, and physical safeguards. Controls are documented in Data Processing Agreements, enterprise agreements, and the publicly available TeamRetro Privacy Policy.

User Access and Licensing:

- Terms of Service (TOS): All users must abide by the TeamRetro TOS, which prohibits sub-licensing or unauthorized account sharing. Each user must have a valid license or be invited under a license holder's account.
- Enterprise Agreements: In some cases, enterprise customers may have separate agreements or service level agreements (SLAs) that override portions of the standard TOS. Where such agreements exist, those terms govern in the event of any conflict.

Security Commitments:

- Principle-Based Architecture: TeamRetro's fundamental design restricts access to data based on a user's role, ensuring that only authorized individuals can view or modify information.
- Documentation and Communication: Security obligations are clearly explained in Data Processing Agreements, enterprise contracts, and the TeamRetro service description.
- Standardized Policies: All security commitments—ranging from encryption standards to incident response procedures—are formalized and maintained centrally, aligned with relevant regulatory requirements.

Operational Requirements:

- Policies and Procedures: The company's internal policies define how systems and data are protected at every stage—from design and development to deployment and day-to-day operations.
- Employee Training and Management: Stringent hiring, onboarding, and training practices ensure that employees understand and adhere to established security and operational protocols.
- Standard Operating Procedures (SOPs): Well-documented SOPs outline the manual and automated processes essential for operating and developing the TeamRetro product, including secure coding practices, patch management, and data backup routines.

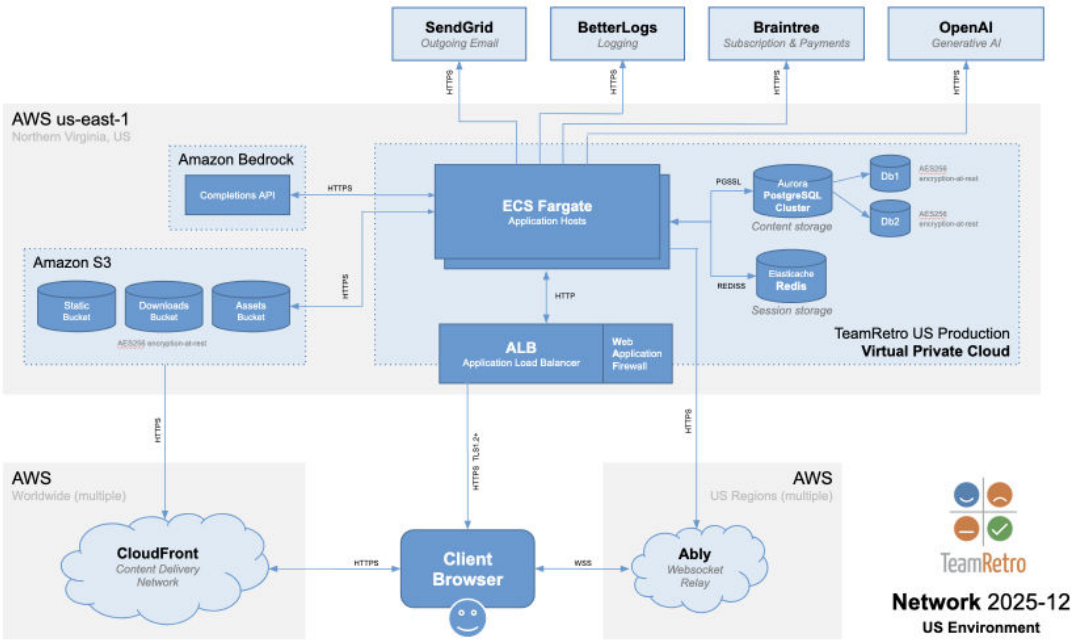
By adhering to these commitments and requirements, GroupMap Technology enables user entities to leverage TeamRetro with confidence that their data is processed securely and in compliance with all relevant legal, regulatory, and contractual obligations.

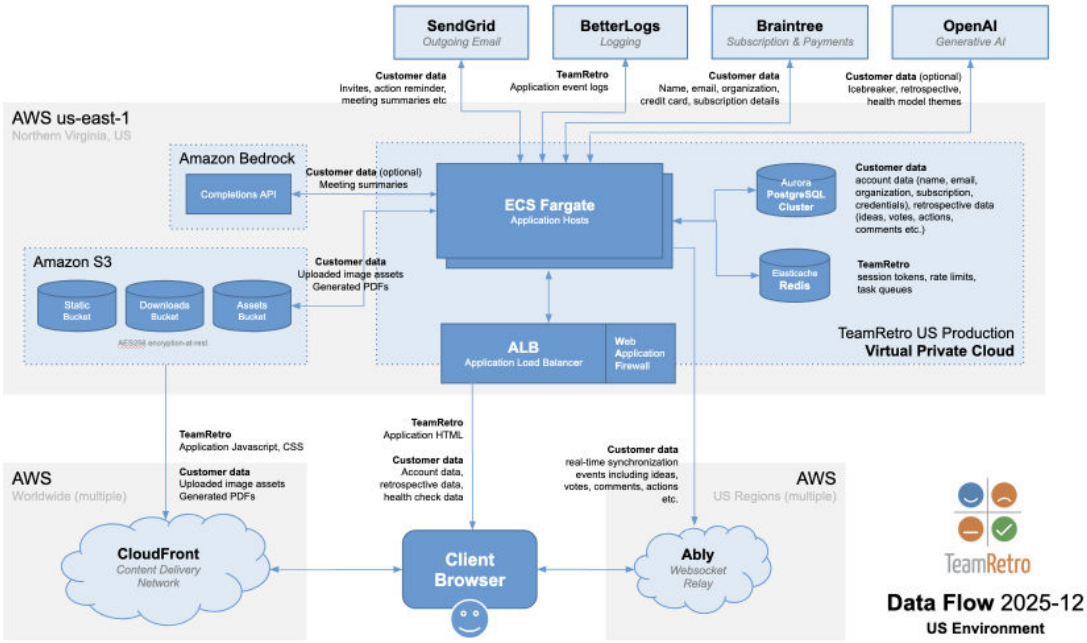
Components of the System

System Architecture

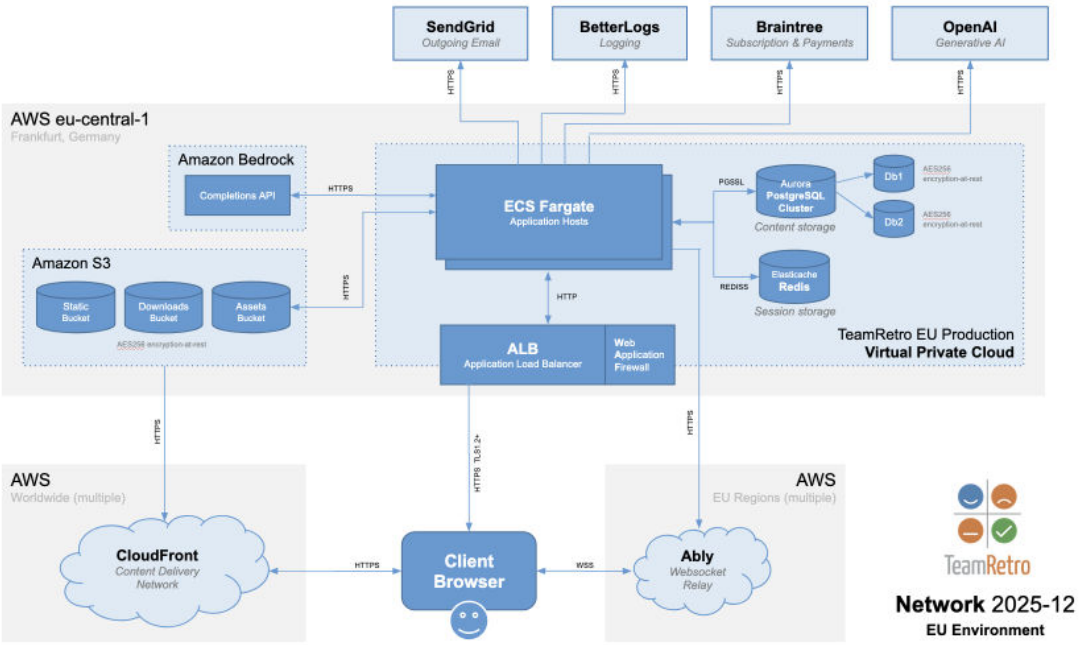
This section provides an overview of the technical components and third-party services that power TeamRetro. It covers the primary hosting environment, sub-processors responsible for infrastructure and platform services, additional software used for operations, and the safeguards in place to protect data.

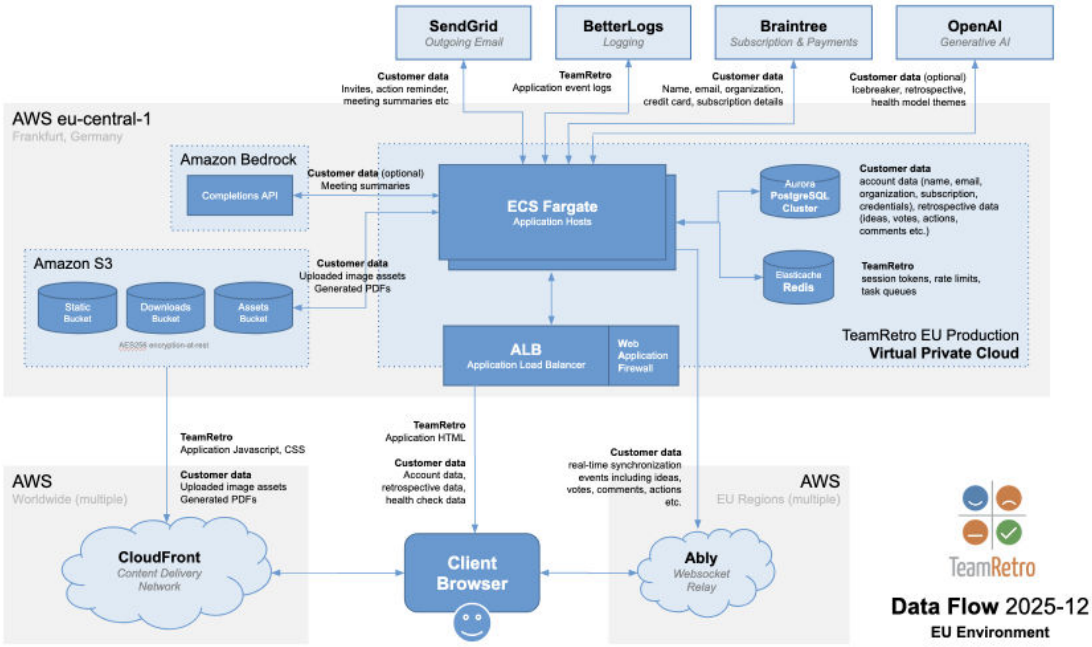
TeamRetro US Environment





TeamRetro EU Environment





GroupMap Technology utilizes industry-leading cloud infrastructure, monitoring, observability, security, and operational tooling providers to support the availability, security, and reliability of the TeamRetro platform. TeamRetro is hosted on Amazon Web Services (AWS), leveraging AWS's global infrastructure to ensure availability, performance, and security.

Key Infrastructure Sub-Processors

In addition to AWS, GroupMap Technology relies on a select group of specialized sub-processors to support TeamRetro's functionality and uptime. Each sub-processor operates under a written agreement that enforces data protection and security obligations:

The following core product sub-processors are used to support the system:

System	Type	Purpose
Ably	Scalable web socket broadcasting	Real-time web socket based data synchronization
BetterStack	Logging (BetterLogs) Monitoring (BetterUptime)	Application logging and uptime monitoring
Datadog	Infrastructure dashboards	Application monitoring, telemetry, and metric services
PayPal	Payment Gateway (Braintree)	Online subscription payments

System	Type	Purpose
Rollbar	Error tracking	Application error tracking and monitoring
SendGrid (Twilio)	Email delivery	Transactional and marketing emails

These monitoring, observability, and operational platforms are used exclusively for operational, performance, and security purposes. They do not store or process personal data for advertising or third-party analytics purposes, in alignment with GroupMap Technology Pty Ltd's 'no third-party analytics cookies' commitment.

AI Synthesis Sub-Processors
The following sub-processors are optionally engaged when customers use TeamRetro's AI synthesis features such as suggested grouping, retrospective and health check meeting summaries, and health check response summaries. AI synthesis features can be globally disabled at the account level at any time.

Software	Type	Purpose
AWS Bedrock	Generative AI	Optional suggested grouping, meeting summaries, and health check response summaries. AWS Bedrock is configured in accordance with AWS enterprise privacy and data handling commitments.

AI Content Generation Sub-Processors
The following sub-processors may optionally be engaged when customers use TeamRetro's generative AI features such as AI-generated retrospective templates, health models, and icebreaker questions. No PII or commercially sensitive information is shared with these sub-processors. These features are optional and can be disabled.

Software	Type	Purpose
OpenAI	Generative AI	Optional AI content generation for retrospective templates, health models, and icebreaker questions

Supporting Software and Operations
GroupMap Technology also uses a range of software tools to manage internal operations and deliver the TeamRetro service effectively. While these do not directly host customer-facing data, they are key to day-to-day business processes. The primary software used to support GroupMap Technology’s system is listed as below:

Software	Purpose
TeamRetro	The Software as a Service System provided to GroupMap Technology customers.
Datadog, BetterStack	System monitoring software used to log events and raise alerts to support system security and availability.
Qualys, Intruder.io	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
Codacy	Code review tool used to conduct static code analysis, monitor code quality and automate code reviews.
GitHub	Source code management tool used for handling version control, CI/CD, and the deployment pipeline.
1Password	Secure password management for employees and contractors.
Bitdefender	Anti-virus software used to protect endpoint devices from malware.
Hexnode MDM	Device management and compliance enforcement tool.
Slack	Communication platform used to collaborate between team members and support business operations.
Ninjio	Security awareness and training management tool.
Prighter	Privacy representation and compliance software used to manage privacy practices in line with data protection laws.
HelpScout	Customer support ticketing and knowledge base software.
Linear	Task and issue management tool for development and support teams.
Google Workspace	Content management workspace used for email, document collaboration, and internal user authentication.
Xero	Accounting and financial operations management tool.
FeatureOS	Product roadmap planning and customer feedback collection tool.

Data Handling and Sub-Processor Oversight

Sub-processors comply with GroupMap's Privacy Policy, ensuring personal data is processed strictly for operational and service-related purposes. No sub-processor is permitted to use personal data for advertising, profiling, or resale.

In addition, GroupMap's responsibilities for handling sub-processors include:

- Written Agreements: All third-party providers sign data protection agreements aligning with high security, confidentiality, and privacy standards.

- Security Review: Evaluating the vendor's documented security posture, including any available certifications or penetration test results.
- Contractual Protections: Ensuring the vendor signs a data protection agreement and commits to using data solely for agreed-upon operational purposes.
- Annual Vendor Review: The company classifies vendors based on risk profile. High-risk vendors undergo an in-depth annual review, during which the company re-validates security controls, certifications, and alignment with its compliance obligations.
- Risk Register Updates: Any new findings or changes in vendor risk status are recorded in a centralized risk register to ensure visibility and timely remediation if necessary.
- Security Controls: The company applies rigorous access control, encryption, logging, and monitoring to safeguard data both in transit and at rest.
- No Advertising Use: In accordance with the GroupMap Technology Privacy Policy, sub-processors are prohibited from using personal or customer data for advertising or third-party analytics.

Architectural Principles

The following principles guide the design and operation of TeamRetro's system architecture:

Resilience

Critical components are redundantly hosted across AWS Availability Zones, safeguarding continuity if a primary component fails.

Security by Design

Infrastructure, application, and data layers are configured with security at the forefront—encryption in transit and at rest, rigorous monitoring, and robust identity and access management (IAM).

Compliance and Transparency

Regular reviews, third-party audits, and adherence to recognized standards (e.g., SOC 2) ensure that GroupMap Technology Pty Ltd meets and exceeds customer and regulatory requirements.

Organizational Structure

GroupMap Technology operates as a lean, globally distributed organization. These primary functional areas include:

1. Executive and Corporate

Scope: Executive leadership, finance, talent acquisition, human resources, and compliance.

Responsibilities:

- Develop and drive overall company strategy and vision.
- Manage financial operations, budgeting, and resource allocation.
- Oversee hiring, onboarding, and professional development.
- Ensure regulatory compliance and corporate governance.

2. Customer Experience (CX)

Scope: Customer support, customer success, and customer delivery.

Responsibilities:

- Provide day-to-day support and training for existing customers.
- Onboard new clients to ensure successful adoption of the TeamRetro Software as a Service System.
- Gather customer feedback and collaborate with product teams to enhance service quality.
- Drive continuous improvements in service delivery and user satisfaction.

3. Product Development

Scope: Product management, user experience (UX) design, software development, and quality assurance.

Responsibilities:

- Plan and prioritize product roadmaps based on customer feedback and market trends.
- Conduct design sprints, user research, and UX optimization.
- Implement and maintain application features, integrations, and system enhancements.
- Ensure consistent high quality through rigorous testing and QA processes.

4. Operations

Scope: Infrastructure, security, reliability engineering, and DevOps.

Responsibilities:

- Manage hosting environments, networking, and cloud-based infrastructure.
- Monitor system performance, capacity, and uptime to meet Service Level Objectives.
- Oversee data security, incident response, and platform resilience.
- Collaborate with development teams to streamline deployment pipelines and automation.

5. Sales

Scope: Business growth, customer retention, and strategic partnerships.

Responsibilities:

- Identify and cultivate new business opportunities across various industries.
- Maintain strong relationships with existing accounts, focusing on retention and expansion.
- Partner with marketing to align messaging and drive lead generation.
- Track sales metrics and forecast revenue to meet organizational goals.

6. Marketing

Scope: Branding, demand generation, and product positioning.

Responsibilities:

- Develop and execute marketing strategies to increase brand awareness and reach.
- Align marketing campaigns with product releases, sales objectives, and target market segments.
- Coordinate content creation, digital advertising, and social media engagement.
- Champion a consistent brand identity across all customer touchpoints.

Each team works collaboratively to deliver a service that meets the needs of a diverse client base. Regular cross-functional meetings, retrospectives, and health checks ensure continuous improvement and alignment with GroupMap Technology's overarching mission.

Data Management

The company defines "Data" for the TeamRetro service to include:

TeamRetro Customer Data:

- Retrospective data (ideas, reactions, groups, votes, comments)
- Health check data (ratings, comments)
- Estimation data (estimates, rounds, imported work items)
- Team action items
- Team agreements
- Custom retrospective and health check templates
- User account information (email addresses, names, avatars, password hashes)
- SCIM groups and users
- User requests (e.g., support or privacy inquiries)

Reports and Logs:

- Activity logs (e.g., user actions, administrative events)
- Admin logs
- API logs
- Error logs
- Integration logs
- System logs

Supporting Data:

- Quotes, invoices, and contracts
- Payment history
- Customer queries, support tickets, and feature suggestions

Reporting Capabilities

Reports can be viewed in the TeamRetro application and are downloadable in electronic Adobe Acrobat (PDF), Markdown (MD), 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:

Client Data	Reporting Options
Retrospective Data	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, MD) 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)
Estimations Data	Estimation summary (PDF, MD) Estimation report (CSV, XLSX)
Team	Teams report (CSV, XLSX) Team activity report (CSV, XLSX) Individual action report (CSV, XLSX)
Users	Users report (CSV, XLSX)

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 TeamRetro Software as a Service 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 include 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. GroupMap Technology is committed to safeguarding personal information in accordance with relevant privacy laws and the TeamRetro Privacy Policy. Below are the key practices:

TeamRetro

Privacy Policy and Consent

- Policy Presentation – Data subjects and Data Controllers are shown the TeamRetro Privacy Policy and Terms of Service upon account creation or invitation acceptance.
- Policy Coverage – The Privacy Policy explains how personal data and intellectual property are collected, used, retained, disclosed, and anonymized.
- Contact Information – The Privacy Policy identifies the assigned Privacy Officer, UK and EU Representative, along with the primary privacy@teamretro.com email address for inquiries.

Collection of Personal Information

- Personal Data: TeamRetro collects the user's email address, full name, and IP address for account setup and basic functionality. Additional optional details (e.g., avatars, language preferences) may also be stored.
- User-Generated Content: If individuals choose to include personal information in retrospectives or health checks, it remains visible only to authorized participants. TeamRetro does not sell customer personal data.

Data Retention

- Ongoing Usage: Data remains active in TeamRetro for the duration of the user's subscription or trial.
- Trial Accounts: Automatically deleted 365 days after the trial ends, unless converted to a paid subscription.
- Canceled Paid Accounts: Customer data is retained for up to 365 days post-cancellation, unless a legal requirement mandates otherwise.
- Backups: Encrypted backups are maintained for up to 30 days for disaster recovery.
- Transaction/Billing Data: May be retained up to 7 years to satisfy legal or financial obligations.

Requesting Data Deletion or Export

- User Rights: Data subjects can request account deletion or personal data export by contacting privacy@teamretro.com or via in-app settings.
- Response Time: Requests are addressed within legally required timelines and in accordance with the TeamRetro Privacy Policy.

Data Usage and Sharing

- Purpose Limitation: Personal data is used solely for providing and improving the TeamRetro service (e.g., facilitating retrospectives, health checks, analytics, and troubleshooting).
- No Third-Party Advertising: TeamRetro does not use or share personal data for advertising or third-party analytics cookies.
- Authorized Sub-Processors: Certain third parties (e.g., hosting providers, payment processors) operate under Data Protection Agreements that align with TeamRetro's privacy, security, and confidentiality commitments.

- Compliance with Law: TeamRetro may disclose data if required by law, or if necessary to protect rights, property, or safety.

Security Measures

- Encryption: All data in transit uses SSL/TLS. Sensitive data at rest (e.g., password hashes) is protected by strong cryptographic methods.
- Hosting: TeamRetro uses AWS with robust physical and environmental controls.
- Administrative Controls: Access is restricted on a least-privilege basis, with continuous monitoring for potential security events.

Security Policies and Procedures

The company maintains a set of formal IT policies and procedures that govern all aspects of security for the TeamRetro service. These policies cover physical security, logical (access) security, computer operations, change control, data communications standards, and more. All teams—employees, contractors, and approved vendors—are required to adhere to these policies, which are centrally stored on the company intranet.

Physical Security Controls

AWS Data Centers

The critical infrastructure and data of TeamRetro is hosted on AWS. There are no trusted local office networks. As such, AWS is responsible for the key physical security controls that support the System. AWS holds multiple certifications that validate the design and operating effectiveness of its physical security controls.

Shared Responsibility

Since AWS provides Infrastructure-as-a-Service (IaaS), GroupMap Technology relies on AWS for data center environmental controls such as fire suppression, uninterruptible power supplies (UPS), and secure access control systems.

Logical Access Controls

Role-Based Access Control (RBAC)

GroupMap Technology implements a role-based security architecture. Each user must be identified and authenticated before accessing any system resources. Access rights are provisioned based on a “least privilege” principle, tied to job responsibilities. Google Workspace authentication software is used for identity management and single sign on.

Multi-Factor Authentication (MFA)

All employees and contractors are required to use MFA for critical systems (e.g., AWS, GitHub, production servers). Passwords alone are insufficient for production access.

Google Workspace Single Sign-On (SSO)

Internal corporate systems, including Google Workspace, enforce password complexity and expiration settings. Employees log in via Google Workspace credentials or other approved SSO solutions. Systems not covered by Google Workspace have separate authentication that meets or exceeds the corporate password policy.

Onboarding and Termination

- Onboarding: New hires undergo a documented process that includes background checks (where legally permissible), assignment of roles, and approval of access.
- Role Change: When an employee's role changes, access is reviewed and adjusted appropriately.
- Offboarding: Upon termination, accounts are disabled immediately, and access roles are removed. The security team documents these changes in the access management system.

Session Lock and Timeout

Employee devices must auto-lock after 15 minutes of inactivity, in accordance with the Information Security Policy.

User Access Review

GroupMap Technology's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access management processes are followed to ensure access rights are reviewed annually 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.

Network Security

Automated and annual 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, monthly testing for and remediation of technical vulnerabilities, and applying network controls like web application firewalls and event monitoring to prevent and detect unauthorized activity.

Endpoint Device Management

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. Hexnode mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

Data Backup and Recovery

Daily Encrypted Backups

TeamRetro data is automatically backed up on a daily basis via AWS Backup. All backups are encrypted at rest. Backup jobs are monitored for completion and any exceptions are immediately investigated.

Retention Period
Encrypted backups are retained for up to 30 days for disaster recovery purposes. Production data associated with canceled accounts is retained for up to 365 days (or as otherwise agreed) in accordance with the TeamRetro Terms of Service and Privacy Policy.

Recovery Testing
Backup and restoration procedures for the System are defined and followed. Backup and recovery procedures are tested annually to verify that data can be successfully restored within required time frames.

Incident Response and Business Continuity
Incident Management Policy
A formal Incident Management Policy outlines how to detect, classify, and respond to incidents, including security, privacy, or any suspected data breach. Incidents must be reported promptly to security@groupmap.com.

Incident Severity Levels
Incidents are categorized based on factors such as number of users affected, potential legal or contractual violations, and confirmed data breaches. Each category has specific escalation procedures and communication requirements.

Post-Incident Review
A post-incident review is conducted within 72 hours of resolution to identify root causes and corrective actions. This review process helps drive continual improvement.

Disaster Recovery and Business Continuity Plans

- Redundant Infrastructure: Critical components run in multiple AWS Availability Zones.
- Plan Testing: The disaster recovery plan and business continuity plan are tested annually, with outcomes documented and updates made as necessary.
- Capacity Monitoring: Resource usage such as CPU, memory and network use, are continuously monitored to ensure consistent performance and availability.

Change Management
Documented Software Development Life Cycle (SDLC)
GroupMap Technology operates a defined process for software development with supporting policies and procedures. GroupMap Technology follows a documented SDLC policy with a structured change management process. Key elements include:

Ticketing System

All changes—whether new features, bug fixes, or infrastructure updates—are tracked in a ticketing system (e.g., GitHub, Linear). Each ticket includes details on the scope of work, associated risks, and testing requirements to support GroupMap Technology's System and objectives.

Peer Review
Code changes undergo peer review before merging into main branches. Developers review each other's commits, focusing on potential security, privacy, or performance issues.

Environment Separation
Changes are first deployed to a development environment for initial testing, then promoted to staging for final validation. Only after successful staging verification and managerial approval are changes promoted to production. This multi-environment approach reduces the risk of introducing defects into live systems.

Approvals and Signoffs
Major or high-risk changes require additional signoffs from the product owner or security lead. This ensures alignment with organizational objectives, including security and compliance standards.

Automated Testing and CI/CD
GroupMap Technology employs continuous integration and continuous deployment (CI/CD) pipelines that automatically run unit tests, static code analysis, and integration tests to catch issues early in the development cycle.

Version Control
GitHub version control software is used to maintain a history of all changes, including roll-back capabilities. Management approvals are required before promoting code to production.

Patch Management
Validation and Deployment
Patch deployment follows GroupMap's documented change management procedures. Proposed patches are tested in a staging environment to ensure stability and compatibility. After successful testing, changes are approved and deployed through the documented change management process.

Penetration Testing and Vulnerability Scanning
Third-Party Penetration Testing
GroupMap Technology engages external security experts to perform annual penetration tests. These tests evaluate the resilience of both network and application layers against potential threats.

Ongoing Vulnerability Scans
Automated vulnerability scans run monthly (or more frequently as needed) to identify new or emerging weaknesses. Retests and on-demand scans occur after major changes or significant findings.

Remediation
Vulnerabilities identified during scans or penetration tests are remediated according to severity. Critical issues receive priority patches, typically within 48 hours.

Data Transmission Security

Encryption in Transit
All data transmitted between user browsers and the TeamRetro service is encrypted using SSL/TLS. This prevents interception or tampering by unauthorized parties.

Firewalls and Network Segmentation
AWS infrastructure includes web application firewalls, Virtual Private Clouds (VPCs), and network access controls. Unapproved traffic is denied by default.

Remote Access Security

Access Logging and Monitoring
Connection logs are maintained for auditing purposes. Anomalous access patterns trigger alerts that are reviewed by the security team.

System Monitoring
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.

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.

Control Environment

The control environment at GroupMap Technology reflects a culture of integrity, ethical values, and dedication to competence. It provides the foundation on which the company designs, implements, and monitors internal controls. Key elements include:

Integrity and Ethical Values

- Ethical Standards: Management promotes ethical and behavioral standards through policy statements, codes of conduct, and by example.
- Acknowledgment of Policies: All staff (including contractors) are required to sign an acknowledgment form confirming their understanding of applicable policies and their commitment to follow all stated procedures.
- Confidentiality: A confidentiality agreement is embedded in the Employee Handbook, reinforcing obligations to safeguard proprietary and client data.
- Background Checks: Pre-employment background and police checks are performed where legally permissible, helping ensure the integrity of the workforce.

Commitment to Competence

- Defined Skill Requirements: Management outlines the knowledge, skills, and competencies needed for each role, documenting them in written position descriptions.
- Ongoing Training: Employees receive training to maintain and develop required skill levels for their positions.

Management's Philosophy and Operating Style

- Executive Oversight: Management and executive committees hold regular meetings to discuss major initiatives, issues affecting the business, and actions needed to maintain privacy and security standards.
- Customer-Centric Focus: A commitment to privacy, security, and user satisfaction is woven into product design, development practices, and daily operations.
- Regulatory Awareness: Executive management remains informed about regulatory or industry changes that may affect services or operations.

Organizational Structure and Assignment of Authority and Responsibility

- Clear Reporting Lines: GroupMap Technology maintains an organizational chart outlining functional areas and chains of command. This chart is updated and communicated as roles evolve.
- Defined Roles: Individual and team responsibilities are clearly assigned so that personnel understand how their actions contribute to the organization's overall objectives.
- Authorization Hierarchies: The company uses formal policies to guide decision-making authority, ensuring responsibilities are delegated appropriately and overseen effectively.

Human Resource Policies and Practices

- Hiring and Onboarding: Background checks, confidentiality acknowledgments, and orientation sessions are part of the standard onboarding process.
- Performance Evaluations: Employees receive annual evaluations to review performance, set objectives, and address training needs.
- Termination Procedures: A documented termination checklist ensures that departing employees have their access rights revoked and return company assets promptly.

Risk Assessment

GroupMap Technology maintains a formal risk register that documents identified risks, potential impacts, likelihood of occurrence, and assigned remediation owners. This risk register is reviewed at least annually—or sooner if significant changes occur in the environment or threat landscape—to ensure controls remain effective. The review process includes:

- Risk Identification: Considers a range of operational, strategic, compliance, and product-related risks, such as changes in the environment, emerging technologies, evolving business models, and shifts in regulatory requirements.
- Risk Analysis: Evaluates how these risks could affect objectives, setting acceptable tolerance levels and designing controls to mitigate or manage them.
- Ongoing Oversight: Senior managers and the executive committee monitor risk-related initiatives, ensuring alignment with corporate strategy and stakeholder interests.

Integration of Risk Assessment with Controls

Risk assessment findings directly inform the design and operation of internal controls. Where potential gaps or vulnerabilities are identified, management implements or adjusts controls to address them. These controls are tested and refined periodically to confirm they remain effective as business or regulatory conditions change.

Information and Communications Systems

GroupMap Technology's Information and communication practices ensure accurate and timely exchange of data necessary to plan, execute, and monitor organizational activities:

- Internal and External Channels: Policies, procedures, and system updates are communicated through formal documentation, email announcements, and approved internal collaboration tools.
- Operational Meetings: Teams hold weekly meetings to address operational issues, share updates, and review new policies or strategic initiatives. Monthly retrospectives and annual health checks support continuous improvement at the organizational level.
- Systems and Reporting: Automated and manual data collection systems (outlined in the Description of Services) feed into management reports that guide decision-making and risk mitigation.

Monitoring Activities

GroupMap Technology performs monitoring to verify that controls operate effectively and continue to meet business and regulatory requirements. Monitoring occurs through:

Ongoing Monitoring

- Quality Assurance Checks: Regular reviews ensure processes align with documented policies.
- Management Involvement: Active oversight by senior leadership helps detect any deviations and initiates corrective actions promptly.

Reporting of Deficiencies

- Issue Tracking: An internal tracking tool documents identified control deviations and their severity.
- Escalation: High-risk issues receive immediate attention, with required remediation steps logged and monitored until resolution.
- Annual Risk Meetings: Management reviews reported deficiencies, effectiveness of corrective actions, and updates to policies or procedures.

Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the executive leadership team, for ensuring appropriate actions are completed in a timely manner.

Changes to the System in the Last 12 Months
No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Incidents in the Last 12 Months
No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Criteria Not Applicable to the System
All Security, Availability, Confidentiality, and Privacy Trust Services Criteria were applicable to GroupMap Technology's TeamRetro Software as a Service System.

Subservice Organizations
This report does not include the cloud-based Infrastructure-as-a-Service (IaaS) provided by 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. TeamRetro utilizes AWS data-centers in Northern Virginia, United States (us-east-1) and Frankfurt, Germany (eu-central-1).

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 Trust Services 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 – AWS		
Category	Criteria	Control
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	Policies and procedures are established and followed to restrict physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers.
	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	Procedures are established and followed to manage environmental protections within the data centers that house network, virtualization management, and storage devices supporting cloud hosting services where the system resides.

GroupMap Technology management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, GroupMap Technology performs monitoring of the subservice organization controls including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

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 Trust Services 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 Trust Services 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 their contractual obligations to GroupMap Technology. In the event of a security incident affecting their system account, the user entity should report incidents immediately to security@groupmap.com. It is recommended that customers enable Single Sign-On (SSO) and SCIM provisioning for improved account security and review access logs periodically.
- Notifying GroupMap Technology of changes made to technical or administrative contact information.
- Ensuring TeamRetro user login additions and changes are authorized prior to being enacted.
- Ensuring TeamRetro user logins are removed in a timely manner upon termination.
- Reviewing TeamRetro user logins on a periodic basis to ensure access is restricted to authorized and appropriate individuals.
- Ensuring privileged roles on their TeamRetro account, administrator and owner roles, are approved by appropriate personnel prior to being enacted.
- Ensuring the supervision, management, and control of the use of TeamRetro by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize TeamRetro.
- Immediately notifying GroupMap Technology of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

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.

Recommended Security Practices for User Entities

GroupMap Technology recommends the following controls and practices for user entities of the TeamRetro Software as a Service System. The following controls and practices are for guidance only and are not required for the achievement of the service commitments and system requirements described in this report:

- It is recommended that user entities configure Single Sign On via their own identity provider (where available) and require SSO login for their TeamRetro account.
- It is recommended that user entities configure SCIM automated provisioning (where available) for their TeamRetro account.
- It is recommended that user entities configure IP address allowlisting (where available) to restrict access to their TeamRetro account to approved network ranges.