TAC Security Inc.
1390 Market, St #200,
San Francisco, CA 94102, USA

Mailmeteor
28 RUE ALBERT
75013 PARIS, FRANCE

28th April 2022

To: Mr. Corentin Brossault
Google Project ID: 1008170693301

TAC Security has verified the application's use of the following restricted Google API scope:
https://www.googleapis.com/auth/gmail.readonly

From 12th April 2022 through 15th April 2022 TAC Security with a retest from 19th April 2022 through 21st April 2022 conducted a security assessment and document review of the https://mailmeteor.com produced by Mailmeteor. We assessed the application, supporting infrastructure and Mailmeteor answers in a self-assessment questionnaire.

Vulnerabilities were reported via ESOF Appsec by TAC Security to Mailmeteor. Vulnerability reports are monitored by Mr. Corentin Brossault.

This testing was undertaken as a part of the Google Cloud Platform OAuth API Verification and should not be read as a comprehensive penetration test or maturity assessment. The purpose of the engagement was to identify security issues with the https://mailmeteor.com and infrastructure during the time allocated to us. TAC Security used automated and manual testing as well as review of the Self-Assessment Questionnaire filled out by https://mailmeteor.com and associated documentation.

This letter confirms that the testing of the https://mailmeteor.com platform application and supporting infrastructure has been completed and that all issues with a Critical or High-risk finding have been remediated. https://mailmeteor.com management has received a report with detailed findings and recommendations from this engagement.

The testing followed the requirements as described in the OAuth API Verification FAQ as last updated on 19th October 2021. These requirements are detailed in Appendix A at the end of this letter. This letter is valid until 28th April 2023.

Signed,
Akash Joshi Akash Joshi Digitally signed by Akash Joshi Date: 2022.04.29 01:11:05 +05'30'
Director ESOF AppSec
TAC Security

TAC Security Inc.
1390 Market, St #200,
San Francisco, CA 94102, USA

Appendix A

1. External Network Penetration Testing: Identify potential vulnerabilities in external, internet facing infrastructure, systems such as the following:
   - Discovery and enumeration of live hosts, open ports, services, unpatched software, administration interfaces, authentication endpoints lacking MFA, and other external facing assets
   - Automated vulnerability scanning combined with manual validation
   - Brute-forcing of authentication endpoints, directory listings, and other external assets
   - Analysis of potential vulnerabilities to validate and develop complex attack chaining patterns and custom exploits
   - Potential exploitation of software vulnerabilities, insecure configurations, and design flaws

2. Application Penetration Testing: Identify potential vulnerabilities in application that access Google user data such as the following:
   - Real-world attack simulation focused on identification and exploitation
   - Discovery of attack surface, authorization bypass, and input validation issues
   - Automated vulnerability scanning combined with manual validation
   - Exploitation of software vulnerabilities, insecure configurations, design flaws, and weak authentication
   - Analysis of vulnerabilities to validate and develop complex attack chaining patterns and custom exploits
   - Verify the ability for users to delete their account with no external indication that the user or user's content is accessible.

3. Deployment Review: Identify exploits and vulnerabilities in developer infrastructure such as the following:
   - Gathering all available configuration settings and metadata as well as manual techniques to build a profile of the cloud environment
   - Analyzing collected information to identify any gaps or deviations from accepted cloud security best practices
   - Manually examining configuration settings to locate anomalies and issues such as weak IAM policies, exposed storage containers, poorly defined security groups, insecure cloud services usage, and insecure key management
   - Exploitation of vulnerabilities, insecure configurations, design flaws, and weak authentication – as needed
   - Verify storage of OAuth tokens is encrypted and encryption keys and secrets are stored in a hardware security module or equivalent strength key manager
   - Ensure developer access to the deployment environment is secured with multi-factor authentication

4. Policy and Procedure Review: Review and examine the efficacy of information security policies and procedures such as the following:
   - Incident Response Plan: Establishes roles, responsibilities, and actions when an incident occurs
   - Risk Management Policy: Identifies, reduces, and prevents undesirable incidents or outcomes
   - Vulnerability Disclosure Program: Provides a means for external parties to report vulnerabilities
   - Information Security Policy: Ensures that all users comply with rules and guidelines related to the security of the information stored digitally at any point in the network
   - Privacy User Data Detection: Ensures that users can delete their accounts and related user data by demonstrating an account deletion if relevant.