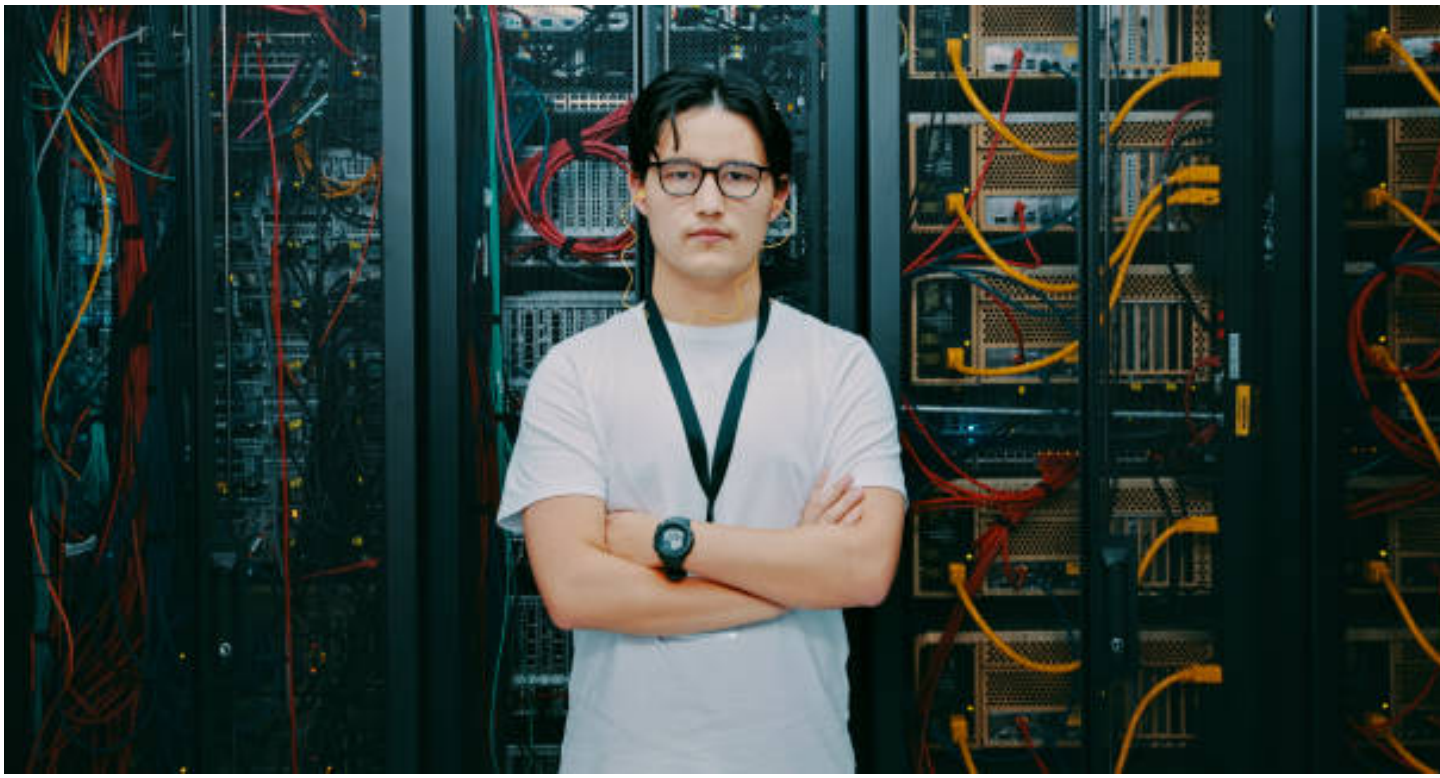
mailmeteor

Mailmeteor

Security Whitepaper



Disclaimer

The content contained herein is correct as of October 2024, and represents the status quo as of the time it was written. Mailmeteor's security policies and systems may change going forward, as we continually improve protection for our customers.

Make sure to regularly check our Privacy Policy and Security Center to stay up to date.

Information Security Policy

Mailmeteor's security and privacy-focused culture

Mailmeteor has created a vibrant and inclusive security and privacy-focused culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and events to raise awareness.

Employee background checks

Before someone joins our staff, Mailmeteor verifies their education and previous employment, and when necessary performs internal and external reference checks.

Security training for all employees

All employees undergo security training as part of the orientation process, and throughout their careers at Mailmeteor. During orientation, new employees also agree to our privacy policy, which highlights our commitment to keeping customer information safe and secure. Depending on their role, employees participate in additional training on specific aspects of security. Software Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques, and more.

Security and privacy events

Security and privacy are an ever-evolving area. It's with this in mind that our employees participate in regular conferences, to raise awareness and drive innovation in security and data privacy.

Audit and compliance

Data protection regulations place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and how security incidents will be managed. To ensure that Mailmeteor remains at the highest level of security,

we regularly check our security procedures and conduct internal and external audits. And we make the results of these analyzes available on our site.

Data Usage

Limited Purposes

Mailmeteor manages data on behalf of its users, including personally identifiable information such as email addresses. Our activity is focused on sending emails and we try to provide the best deliverability experience. That's why we don't sell or transfer data to third parties or even scan it for advertising purposes.

Administrative Access

We've designed our infrastructure to limit the number of employees that have access to users' data and restrict who has access based on the purposes of that access. Access is controlled via IAM (Identity Access Management) policies and automatically removed for departing employees. Mailmeteor also employs extensive security measures to minimize access:

- restricts access to employees who have a business purpose to access personal data.
- logs employee access to systems that contain personal data.
- only permits access to personal data by employees who sign in with Google Sign-In and 2-factor authentication.

Data Encryption

Mailmeteor encrypts user data in transit using HTTPS and logically isolates customer data. In addition, data is encrypted at rest using server-side encryption. Data and metadata are encrypted under the 256-bit Advanced Encryption Standard. The cryptographic keys are managed by our hosting solution (Google Cloud) using the same hardened key management systems that they use for their own encrypted data, including strict key access controls and auditing.

Data Retention

Mailmeteor stores users' data in accordance with our data retention policy. When storing data, Mailmeteor always strikes a balance between providing the best user experience and also the risk that this data poses in terms of security. In all cases when we keep data, we do so in accordance with any limitation periods and records retention obligations that are imposed by applicable law.

Data Deletion

Mailmeteor ensures that users are able to delete their accounts - and related data - on demand.

Access and Authentication

Google Sign-In

Our users can access our applications using Google Sign-In only. This helps mitigate the risks of password management and leaks. Our users can strengthen account security by using 2-step verification and security keys in their own Google accounts.

Single sign-on (SAML 2.0)

Mailmeteor supports SSO through our usage of Google Sign-In. This helps large enterprises to benefit from Google Workspace's single sign-on (SSO) solution and secure even further their organizational usage of our applications.

Vulnerability Disclosure Program

Mailmeteor fosters an open relationship with the security community, as we recognize the importance of application and data security. Our Vulnerability Disclosure Program demonstrates our commitment to security as a key value and to

uphold our legal responsibility to good-faith security researchers who choose to help validate our applications.

Qualifying vulnerabilities

Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be within the scope of the program. Common examples include:

- Cross-site scripting;
- Cross-site request forgery;
- Mixed-content scripts;
- Authentication or authorization flaws;
- Server-side code execution bugs.

Reporting a Vulnerability

Any vulnerabilities you may find should be reported to our security team via an email sent to the following address: security@mailmeteor.com. To ensure confidentiality, we encourage you to encrypt any sensitive information you send us.

Bounties

The decision to pay a reward is entirely at our discretion. You must not violate any law. You are
responsible for any tax implications or additional restrictions depending on your country and local law. We reserve the right to cancel this program at any time.

Disclosure

In order to protect our customers, TINT requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.

Incident Management

Incident response is a key aspect of Mailmeteor's overall security and privacy program. We have a rigorous process for managing incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

Mailmeteor's incident response program is managed by expert incident responders across many specialized functions to ensure each response is well-tailored to the challenges presented by each incident.

Detection and Analysis

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of this procedure.

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change. For an electronic incident, Mailmeteor will perform static and dynamic analysis of malicious code, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced.

These analyses can be performed either manually or utilizing automated tools depending upon the situation, timeliness, and availability of resources.

An incident will be categorized as one of four severity levels. These severity levels are based on the impact. The below table provides a listing of the severity levels and a definition of each severity level.

0 (Low)	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions. Users' data or Mailmeteor's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting
3 (Extreme)	Incident where the impact is catastrophic. Examples may be a shutdown of all [municipality or county name]'s network services. Users' data or Mailmeteor's proprietary or confidential information has been compromised and published in/on a public venue or site.

Remediation

Mailmeteor's security team is responsible for eradication and will document all eradication activities during an incident. Remediation efforts for a security incident involve the removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Post-Incident Activity

Following the successful remediation and resolution of a data incident, our security team evaluates the lessons learned from the incident and shares its results with the rest of the company.

When the incident raises critical issues, Mailmeteor's CIO may initiate a post-mortem analysis. During this process, our security team reviews the cause(s) of the incident and identifies key areas for improvement. In some cases, this may require discussions with different product, engineering, and operations teams and product enhancement work.

If follow-up work is required, our security team develops an action plan to complete that work and assigns project managers to spearhead the long-term effort. The incident is closed after the remediation efforts conclude.

Risk Management

Risk management refers to all activities performed by Mailmeteor to anticipate, identify, assess and control the uncertainties which may impact Mailmeteor's ability to achieve its aims, objectives and opportunities. These will range from organization-wide to specific projects or programs, to the individual.

The risk management policy aims to demonstrate that Mailmeteor is acting appropriately to anticipate risks; assess risks; avoid excessive risk; embrace necessary or desirable risks with appropriate safeguards; that its response to risk, whether by insurance, control measures, or avoidance, is proportionate and effective; that responsible employees are equipped to take risk-based decisions with confidence; and that we are intelligent in applying our risk appetite.

Managing Risks

Risks are an everyday part of our activities. Our operations involve multiple partnerships, challenging environmental, organizational contexts and extensive geographic scope. The realization of our mission and strategy depends on our ability to recognize risks and define suitable measures for their treatment.

Monitoring and Learning

Mailmeteor monitors the risks on the Strategic Risk Register, especially those with a “High” risk score. We also learn from our experience in risk management and seek to share issues, and ideas with staff to enable them to work effectively in a risk-based manner. This includes learning from those risks that we take on knowingly, where we believe that we could secure significant benefits if the risks are handled responsibly.

Internal Controls

Internal controls encompass a review of the risks inherent in each activity. Mailmeteor’s approach includes regularly reviewing its operational risks such as changes to our codebase, third-party modules and dependencies updates, and access controls to development and production data.

Also, we rely on multiple third-party solutions to make sure we receive alerts when a new risk has been identified and remediations can take place in a timely manner.

External Controls

Mailmeteor commits to regular audits performed by qualified third-party security assessor firms.
These external controls help keep Maillmeteor users’ data safe by verifying that our applications demonstrate capability in handling data securely. External assessments happen at least once a year and take place aside from our Vulnerability Disclosure Program.

Conclusion

The protection of your data is a primary design consideration for all of Mailmeteor's infrastructure, products, and personnel operations. We believe that Mailmeteor can offer a level of protection that very few emailing platforms aim to reach.

For these reasons and more, over three million professionals across the globe trust Mailmeteor with their most valuable asset: their emails. Mailmeteor will continue to invest in its security to allow you to benefit from our services in a secure and transparent manner.