Mailmeteor’s Risk Management Policy

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.

Disclaimer

The content contained herein is correct as of April 2022, 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.