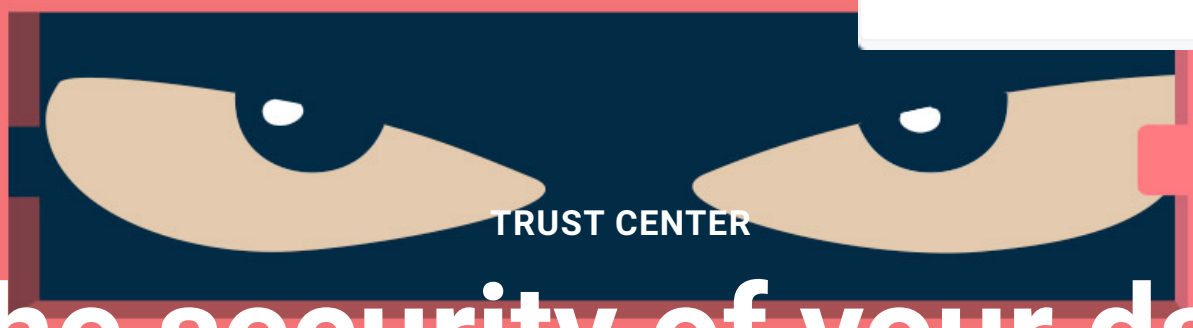
We use cookies to provide the best site experience. Find out more



TRUST CENTER

The security of your data matters to us

We are committed to securing our customers' data to the highest degree. Campaign Monitor provides a service to over 200,000 companies across 180 countries. Our customers include healthcare providers, educational institutes, financial services, and governmental agencies; small and medium sized businesses who trust us with some of their most sensitive information. That's why trust is the foundation of our privacy and data security promise to our customers.

Operational security

Our adaptive, forward-looking measures are our promise to you.

Dedicated security team

We have a dedicated information security team, responsible for securing the application, identifying vulnerabilities and responding to security events.

Data storage and processing locations

We store data in a US-based data center. In addition, we use multiple data processing locations including USA, Australia and Germany. We also use Fastly as an external content delivery network, which is used for content caching. Fastly's locations are available here: https://www.fastly.com/network-map.

Security policies

We have a suite of security guidelines with supporting procedures, which have been aligned with the ISO 27001 standard. Our security documentation is frequently reviewed and updated to reflect changes to our processes made in response to newly identified threats, as well as our commitment to continuous improvement.

We use the NIST Cyber Security Framework to measure our ability to identify, protect, detect, respond and recover from security events.

Awareness and training

All staff and contractors go through a vetting process where they are subject to background checks and confidentiality agreements.

We provide an ongoing program of security awareness training designed to keep all members of staff informed and vigilant of security risks. This includes regular assessment of comprehension to measure the program's effectiveness.

Physical security

We implement physical controls designed to prevent unauthorized access to, or disclosure of, customer data.

Data center controls

We only use state of the art data centers and cloud providers. Our data centers are monitored 24×7 for all aspects of operational security and performance. They are also equipped with state-of-the-art security such as biometrics, sensors for intrusion detection, keycards, and around-the-clock interior and exterior surveillance.

In addition, access is limited to authorized data center personnel; no one can enter the production area without prior clearance and an appropriate escort. Every data center employee undergoes background security checks.

Data center compliance

Our data center provider is certified to the following compliance standards: HIPAA, PCI-DSS, SOC 1 Type 2, SOC 2 Type 2, ISO 27001 and FISMA/NIST.

Our cloud provider has the following certifications: PCI-DSS, ISO 27001, SOC 1 / 2 / 3, IRAP, ISO 27018 and ISO 9001.

Application security

Our application has been designed with focus on security by leveraging OWASP-aligned security principles for software engineering, encryption technologies and security assurance.

Security testing

We use a combination of regular scheduled scans of our application, as well as penetration testing and bug bounty programs, to ensure that every area of our

application has undergone rigorous security testing.

Our scheduled vulnerability assessment scans simulate a malicious user, while maintaining integrity and security of the application's data and its availability.

Security controls

We never give, rent, or sell access to your data to anyone else, nor do we make use of it ourselves for any purpose other than to provide our services. See our full privacy policy for more information.

We store each account's data within a unique identifier, which is used to retrieve data via the application or the API. Each request is authenticated and logged.

Secure code development

We follow industry best practices and standards such as OWASP and SANS. We have separate environments and databases for different stages of the application development. We do not use production data in our test and development environments.

Data encryption

To protect data we encrypt information in transit by supporting TLS 1.0, 1.1 and 1.2. Data at rest is also encrypted using AES-256 encryption.

User access

We put considerable effort into ensuring the integrity of sessions and authentication credentials. Passwords storage and verification are based on a one-way encryption method, meaning passwords are stored using a strong salted hash. Email addresses are validated against a strong salted hash, stored along with the email.

The databases are further protected by access restrictions, and key information (including your password) is encrypted when stored. Data is either uploaded directly into the application using a web browser or uploaded via the API which uses secure transfer protocols.

Logging and cookie management

We use cookies for user authentication. We use session IDs to identify user connections. Those session IDs are contained in HTTPS-only cookies not available to JavaScript.

All key actions on the application are logged and audited, for instance whenever our staff

access an account for maintenance or support functions, such activities are logged so we can refer to them later.

See why 200,000 companies worldwide love Campaign Monitor.

From Australia to Zimbabwe, and everywhere in between, companies count on Campaign Monitor for email campaigns that boost the bottom line.

REQUEST A DEMO

© 2018 Campaign Monitor - Email Marketing Software