ActiveCampaign
DATA PROTECTION AND SECURITY

Your data is unique. Your privacy is valuable. Here's what we do to protect them:

Cutting-edge security protects your data:
Our proactive, offensive security eliminates threats—before alerts are ever triggered

Compliant
ActiveCampaign is heavily focused on GDPR, SOC 2, and HIPAA compliance. We constantly improve our security to go above and beyond compliance standards.

Automated
Security scanning tools help our engineers incorporate security throughout our product development lifecycle. We build in-house tools to scan code, scan infrastructure, and automatically detect anomalous activity.

Proactive
We continuously attempt to hack our own systems. Offensive engagement allows us to find and correct vulnerabilities faster than they can be exploited by malicious parties.

How we go beyond what's expected of modern security:
Alerts aren't enough. We use state-of-the-art techniques to stay ahead of hackers.

Information classification
All our data is classified and restricted, which lets us prioritize the most sensitive information. Single-tenancy architecture means that each person's data is kept separate from everyone else's. Along with secure, world-class data centers, this data separation helps keep your data secure.

Authentication and access security
Personnel have the exact level of access required, and user access is regularly audited to ensure data protection. In keeping with National Institute of Standards and Technology (NIST) requirements, data access is protected by multi-factor authentication, password control, keys, and other best practices.

Access zone security
Our networks use a layered access classification framework to provide data separation. Each client-protected single tenancy data store, whether physical or virtual private cloud, is a fully security-hardened stack that includes endpoint and network threat prevention, application firewalling, and vulnerability scanning.

This copy is provided as a courtesy only and does not constitute legal advice

Secure software development lifecycle
Security is baked into our software development—developers are active participants in securing the code that they write. Security scanning tools and code analysis help them resolve any issues with open-source packaging, misconfigurations, and potential vulnerabilities.

Internal offensive security
Our in-house Red Team engages in continuous penetration testing. We try to break our own production systems every day—so that we can stay ahead of the curve and address potential issues.

Security is built into our software development lifecycle:
Security starts before the first line of code. That's why we bake security into every stage of our software development lifecycle (SDLC).

Secure Thinking
Our developers consider security from day one. We consider common security flaws and exploit techniques at the beginning of our SDLC

Security Scanning Tools
Developers use embedded security scanning tools in their deployment process. Static code analysis and open-source package management let us flag potential issues or vulnerabilities.

Daily Vulnerability Scans
We scan our product daily, to flag and correct potential vulnerabilities as quickly as possible (using dynamic analysis).

Continuous Pen Testing
Every day, we try to hack our own systems. Our offensive security team thinks like hackers to find and address potential issues.

Security Community Experts
We're involved in the security community at the local, national, and international level. Our team consists of active contributors to OWASP.

Security features that meet your unique business needs:
ActiveCampaign gives you full control of your data with features that prioritize privacy and security at every stage of your growth.

Single sign-on

This copy is provided as a courtesy only and does not constitute legal advice

Automatically log into ActiveCampaign through an identity provider without needing a separate set of credentials. SSO means better enterprise security for your business — and better peace of mind for your users since they need to remember fewer passwords.

Multi-factor authentication
We start with trust at ActiveCampaign, so we make multi-factor authentication (MFA) available to every account. We recommend you enable it to help keep your data more secure by requiring verification through SMS and TOTP authenticators.

Session management
Log an ActiveCampaign user out if they are idle for a predetermined period of time. Customize the length of an active session to meet your specific security needs and help keep your account secure and protected from potential compromises.

Security package request form:

We are committed to protecting and safeguarding your data with full transparency into security, privacy and compliance controls at ActiveCampaign. Our security package contains our latest available SOC 2 report, penetration test summary, architecture diagram, and comprehensive security FAQ. If you would like to request the security package, please complete the form found at the link below and we will be in contact with you shortly after.

For cutting-edge security, we built a cutting-edge team:
We built a team with world-class security skills. Our team includes experts with experience in compliance and privacy, risk, threat exposure management, application security, secure cloud and infrastructure, incident response, and red teaming.