Security at Ethos

System security

Security Certifications

Ethos Hub has secured ISO27001 certification and has implemented SOC2 compliance procedures.

Coding Standards and Development

We are aware that a well-built environment requires adherence to high coding standards, as well as tests and code reviews that protect against security breaches. We have strict development processes, and our developers adhere to coding standards that are in accordance with OWASP.

Application Security

System components undergo thorough tests and source code reviews to ensure the security of our application interface and architecture before we apply this code to the production environment.

A stringent vulnerability management process is in place to allow early identification of vulnerabilities and fix them according to predefined timelines based on severity.

Penetration tests by independent, 3rd party suppliers and in-house testers are performed every year.

Static application security testing (SAST) is in place to improve the Ethos Hub Software Development Lifecycle (SDLC).

Access Control

We emphasize a strong access control policy to keep our platform and our customers' data safe. Our AWS EC2 instances are firewall restricted to Ethos IP addresses and SSH access requires authentication with a secure private key which only a few key team members approved by the Ethos Head of Operations have access to.
All team members are required to use two-factor authentication on any cloud platform where it's possible (e.g. AWS, GitHub, etc.).

Patch Management

Ethos cares deeply about the stability and availability of our services. That's why all critical issues are patched immediately.

Data Center

Ethos Hub infrastructure resides within Amazon AWS EC2 private instances (Amazon VPC) with Amazon Enterprise support in place. The Ethos Hub is deployed via Amazon AWS Elastic Beanstalk for auto-scaling and load-balancing to guarantee availability.

Ethos's Hub primary database system is MySQL, using Amazon RDS. The secure database offers failover, snapshots, and backup capabilities of the highest standard to safeguard company data.

Customer Data Security

We are committed to protecting your data and maintaining confidentiality. We employ advanced security practices to keep your data safe and secure.

Data in Transit (Cryptographic Policy)

Every connection between Ethos Hub and a third party service is established in the most secure way that is supported by the given service. We are working with TLS version 1.2, using AES 256 encryption, with an exception for webhooks allowing the use of TLS version 1.0.

Data at Rest

We use the industry-grade and battle-tested bcrypt algorithm to securely hash and salt passwords, so they cannot be read and/or reproduced by anyone - not even us.

We use full-disk encryption with the industry-standard AES-256 encryption algorithm. All services provided by our suppliers or AWS EBS / AWS S3 volumes are encrypted by default. We use AWS Key Management Service (KMS) for managing cryptographic keys. Furthermore, we do not allow customers to supply their own encryption keys.

Customer Best Practices for Security

This section describes what you should or should not do to protect your account most effectively.

You are responsible for maintaining the security of your unique password and account information at all times. Your password must be at least eight characters long, and it must contain at least one uppercase letter, one number, and a special character.

We recommend using strong passwords that rotate, and this can be set up directly in your account.

We do not recommend sharing the credentials of your user account with other colleagues or anyone else, nor do we advise sharing accounts between multiple users.

Privacy Policy

We take comprehensive efforts to protect the privacy of our customers and their data stored within our platform.

For more information on security and compliance, please refer to our trust center: https://www.ethos.co.uk/privacy-policy/

People Operations

Recruiting and Hiring

All employees must agree to company policies before starting their employment (including confidentiality and security policies).

Onboarding Policy

All new team members at Ethos undergo information security awareness training. They are also required to sign nondisclosure and confidentiality agreements, and they are required to acknowledge in writing that they understand and adhere to corporate security policies.

Exit Policy

During the exit processes, all login details for employees who are leaving the company are removed, and SSH keys, VPN access, etc. are deleted.

All data on all electronic devices used by the leaving employee are destroyed.

Every employee must sign a contract during the onboarding process that includes an agreement to maintain confidentiality about business operations and customer details, even after the end of the contract.

Employee Access to Customer Data

Only a few designated Ethos Hub team members are able to access the servers or any sensitive customer data. All attempts to access sensitive data are logged.

Employee Devices

All electronic devices used by Ethos employees have enabled disk-based encryption.

Company Accreditations

Data privacy and security have always been top priorities for Ethos. As we've built our software, maintaining user privacy has always been a key part of our product development, marketing, and company culture.

We have invested heavily in various training and certification programs to ensure that our products and services follow the principles of confidentiality, integrity and availability.

Ethos is committed to achieving the highest of security standards with the proper controls, as defined by industry standards and frameworks on an ongoing basis.

QSL ISO 9001 Quality Management Certification

QSL ISO 14001 Environmental Management Certification

QSL ISO 45001 Health & Safety Management Certification

QSL ISO 27001 Information Security Management Certification

We are a Living Wage Employer

THE MAYOR'S GOOD WORK STANDARD