Lawbrokr Security

Policies and practices

Lawbrokr is committed to ensuring the confidentiality, integrity, and availability of our users' data. We continuously review and improve our security practices to ensure they remain effective in mitigating potential security threats.

Hiring and training

To ensure secure hiring and training of employees, Lawbrokr has implemented the following security measures:

- **Non-disclosure agreements:** Lawbrokr requires all new employees to sign a non-disclosure agreement (NDA) to protect sensitive information and data.
- **Security training:** We provide security training to all new employees to ensure that they are aware of the company's security policies and procedures. The training covers topics such as password security, phishing, and social engineering.
- **Account management:** Lawbrokr monitors access rights to ensure that they are aligned with the company's policies and procedures. We promptly disable access for employees who are no longer employed by the company.

Network security

Lawbrokr utilizes Fly.io, a cloud platform that provides a secure and reliable infrastructure for running global applications. For more complete information on Fly.io security click here.

An overview of the Fly.io security policies and measures are provided below:

- **Network security:** Fly.io uses encrypted communication channels to ensure that data transmitted between applications and the Fly.io platform is secure. It also uses industry-standard protocols such as SSL/TLS to secure connections. Furthermore, Fly.io uses distributed denial-of-service (DDoS) protection to prevent attacks on its network.
- **Application security:** Fly.io uses isolation technologies to ensure that applications are isolated from one another, and it also uses containerization to ensure that applications are running in secure and isolated environments. Additionally, Fly.io provides security features such as secure secrets management and access control to help customers protect their applications.
- **Compliance and certifications:** Fly.io is compliant with several industry-standard regulations such as GDPR, SOC 2 Type 2, HIPPA and ISO 27001. Fly.io also undergoes regular security audits and assessments to ensure that its platform remains secure and compliant with industry standards.

Encryption

All data in transit, as well as data at rest, is encrypted to protect against unauthorized access. We utilize 256-bit AES encryption to secure data stored on our systems, and we implement Transport Layer Security (TLS) 1.2 for data in transit. Encryption controls are reviewed periodically and as new threats emerge.

Payment processing

Lawbrokr is not involved in processing or storing payment card information belonging to our customers. To ensure secure credit card processing, we rely on the services of Stripe, an external payment processing company. Stripe is a certified PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry.

Monitoring and Logging

Lawbrokr monitors and logs all activities on its systems to detect and respond to any suspicious activity. We also regularly review logs to identify potential security breaches.

Secure software development

Lawbrokr employs a secure software development practice to ensure the confidentiality, integrity, and availability of data in software applications.

Threat modeling:
Threat modeling is utilized to identify potential security threats to a software application and determine the best ways to mitigate them. The threat modeling process is conducted at the start of the software development lifecycle and continuously reviewed throughout the development process.

Secure coding practices:
Lawbrokr adheres to coding standards and guidelines, uses secure coding techniques, and avoids common programming errors that could lead to security vulnerabilities. Secure coding practices are integrated into the software development lifecycle and continuously reviewed throughout the development process.

Code review:
Code reviews are conducted through a combination of manual and automated processes. Code reviews are conducted regularly throughout the software development lifecycle to ensure that any potential security vulnerabilities are identified and addressed promptly.

Testing and validation:

Testing and validation are conducted at different stages of the software development lifecycle, including unit testing, integration testing, and acceptance testing. Automated testing tools and techniques help to identify potential security vulnerabilities and reduce the likelihood of security breaches.

Data backup

Lawbrokr maintains regular backups of all data stored on its systems to ensure data can be restored in the event of data loss.

Incident response

Lawbrokr has a documented incident response plan in place and ensures that all employees are trained on the plan. The plan includes roles and responsibilities, communication procedures, and escalation protocols.

Disaster recovery

Lawbrokr has a disaster recovery plan in place to ensure that critical business operations can continue in the event of a natural or man-made disaster.