FusionStak | CloudGavel

CloudGavel Security

At CloudGavel, we prioritize the security of your data and our services. Our commitment to maintaining the highest standards of security is evident in our comprehensive approach to protecting your information. Below is an overview of our security practices, certifications, and commitments.

Security Practices

Data Encryption

- **In-Transit**: We use TLS 1.2+ to ensure data is encrypted during transmission between your devices and our servers.
- **At-Rest**: All data stored in our databases is encrypted using AES-256.

Access Controls

- **Role-Based Access Control (RBAC)**: We implement RBAC to ensure that users have access only to the data necessary for their role.
- **Multi-Factor Authentication (MFA)**: MFA is required for all internal and external access to our systems to provide an additional layer of security.
- **Least Privilege**: Our access policies follow the principle of least privilege, granting only the minimum level of access necessary for job functions.

Network Security

- **Firewalls and IDS/IPS**: We deploy advanced firewalls and intrusion detection/prevention systems to protect our network from unauthorized access and threats.
- **Network Segmentation**: Our network is segmented to isolate and protect sensitive data and systems.

Vulnerability Management

- **Regular Scanning**: We conduct regular vulnerability scans and penetration tests to identify and address potential security weaknesses.
- **Patch Management**: Our systems are routinely updated with the latest security patches to mitigate risks from known vulnerabilities.

Incident Response

- **24/7 Monitoring**: Our security team monitors our systems around the clock to detect and respond to incidents promptly.

- **Incident Management**: We have a robust incident response plan in place to manage and mitigate the impact of security incidents.

Certifications and Compliance

SOC 2 Type I

We undergo regular SOC 2 Type I audits to ensure our security controls meet the highest standards for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality, and privacy.

CJIS Compliance

CloudGavel is compliant with the Criminal Justice Information Services (CJIS) Security Policy. This compliance ensures that we adhere to the stringent security requirements necessary to protect sensitive criminal justice information.

Commitment to Privacy

Data Privacy

Your privacy is paramount. We follow strict guidelines to ensure your data is collected, processed, and stored in accordance with applicable privacy laws and regulations.

Transparency

We believe in transparency regarding our data practices. Our Privacy Policy outlines what data we collect, how we use it, and your rights regarding your information.

Data Retention and Deletion

We have clear data retention policies and provide you with the ability to request the deletion of your data in accordance with applicable laws.

Security Awareness

Employee Training

All CloudGavel employees undergo regular security awareness training to stay informed about the latest security threats and best practices.

Security Culture

We foster a culture of security throughout our organization, encouraging everyone to take responsibility for protecting our customers' data.

Contact Us

If you have any questions about our security practices or need to report a security concern, please contact us at support@cloudgavel.com.