Beast Holdings LLC

Security Statement

Last updated: September 27, 2025

1. Commitment to Security

Beast Holdings LLC is committed to protecting the confidentiality, integrity, and availability of all information assets entrusted to us.

2. Technical Safeguards

Our systems employ SSL/TLS encryption, firewalls, intrusion detection, and secure hosting environments to protect data in transit and at rest.

3. Administrative Safeguards

We enforce least privilege access, conduct quarterly access reviews, and require ongoing staff training on data protection and security practices.

4. Incident Response

In the event of a suspected or confirmed incident, Beast Holdings LLC will investigate promptly, contain the issue, and notify affected parties in compliance with applicable law. Critical incidents are acknowledged within 15 minutes.

5. Backups & Continuity

We maintain weekly encrypted backups, with Recovery Time Objective (RTO) of 24 hours and Recovery Point Objective (RPO) of 24 hours. Quarterly restore tests verify our readiness.

6. Compliance

We comply with PCI DSS requirements for payment processing and adhere to GDPR/CCPA security obligations and other global standards.

7. Shared Responsibility Model

While Beast Holdings LLC secures its systems and data, customers are responsible for safeguarding their account credentials, using secure devices, and reporting suspected issues promptly.

Security: security@beast-llc.com Legal: legal@beast-llc.com
Operations: operations@beast-llc.com Press: press@beast-llc.com

8. Limitations

No system can guarantee absolute security. Users acknowledge inherent risks in online services and agree to use reasonable security practices.

9. Contact

For security inquiries, please contact security@beast-llc.com or legal@beast-llc.com.

Compliant with PCI DSS, GDPR/CCPA data protection standards, and international best practices.