hitchpay

SECURITY WHITEPAPER

How HitchPay protects your money and data

A technical overview of the controls, architecture and governance that secure the HitchPay global finance platform.

Version 1.0 · 2026 · HitchPay Technologies, Inc. · Classification: Public

Contents

1 Executive summary

HitchPay is a global finance platform that gives businesses multi-currency accounts, cross-border payments and corporate cards. Because we move money and hold sensitive data on behalf of our customers, security is engineered into every layer of the platform rather than added as an afterthought.

This document describes the safeguards that protect customer funds and information: encryption of data in transit and at rest, a hardened cloud infrastructure, least-privilege access controls, continuous monitoring, an independently audited control environment, and a mature financial-crime and incident-response program. It is intended for prospective customers, partners and their security teams evaluating HitchPay.

Encryption everywhere · Independent audits · Regulated partners · 24/7 monitoring · Least privilege

2 Security governance & program

Security at HitchPay is owned by a dedicated team that reports to executive leadership, with defined policies reviewed at least annually and approved by management. Our program is built around recognized frameworks and the principle of defense in depth.

- Written information-security, acceptable-use, access-control, data-classification and incident-response policies.
- Mandatory security and privacy training for all employees at onboarding and annually thereafter.
- Background checks for personnel where permitted by law, and confidentiality obligations for staff and contractors.
- Risk assessments performed regularly and after material changes to systems or the threat landscape.

3 Data protection & encryption

In transit

All traffic to and from HitchPay is encrypted with TLS 1.2+ using strong cipher suites. HSTS is enforced and plaintext connections are refused.

At rest

Data is encrypted at rest using AES-256. Encryption keys are managed in a dedicated key-management service with strict access controls and rotation.

Sensitive data handling

- Secrets and credentials are stored in a managed secrets vault, never in source code.
- Card data is handled within a PCI-DSS scoped environment; sensitive identifiers are tokenized where possible.
- Data is classified and access is granted on a need-to-know basis according to its sensitivity.

4 Application & product security

Security is embedded across the software development lifecycle so that vulnerabilities are found and fixed before they reach production.

- Mandatory peer code review and protected branches for every change.
- Automated static analysis (SAST), dependency and secret scanning in the CI/CD pipeline.
- Regular dynamic testing and independent third-party penetration tests, with findings tracked to remediation.
- Input validation, output encoding and parameterized queries to defend against injection and cross-site scripting.
- Multi-factor authentication, rate limiting and anomaly detection on customer-facing endpoints.

5 Infrastructure & network security

HitchPay runs on reputable cloud infrastructure providers that maintain their own leading security certifications. Our environment is designed for isolation, resilience and observability.

- Network segmentation with private subnets; production systems are not directly exposed to the public internet.
- Web application firewall and DDoS protection at the edge.
- Infrastructure-as-code with peer-reviewed, auditable changes and hardened baseline images.
- Centralized, tamper-resistant logging with continuous monitoring and alerting.
- Separate development, staging and production environments with no shared credentials.

6 Identity & access management

Access to systems and data follows the principle of least privilege and is granted only for as long as it is needed.

- Single sign-on and enforced multi-factor authentication for internal systems.
- Role-based access control, with privileged access approved, time-bound and logged.
- Access reviews performed on a recurring basis and revoked promptly on role change or departure.
- Customer accounts support MFA, granular team permissions and full audit trails.

7 Safeguarding customer funds

HitchPay is a financial technology company, not a bank. Banking services are provided by our partner bank, Lead Bank, Member FDIC. Customer funds are held in dedicated accounts at regulated partner banks, kept separate from HitchPay's operating funds and reconciled daily.

- Eligible USD balances are held at an FDIC-member partner bank and may qualify for pass-through FDIC insurance, subject to the terms of the applicable deposit arrangement.
- Foreign-exchange and payment services are powered by licensed money-transmission and payment partners.
- Segregation of duties and multi-step approvals govern the movement of funds.

8 Compliance, certifications & financial crime

HitchPay maintains an independently assessed control environment and a risk-based financial-crime program.

Assurance

SOC 2 Type II and PCI DSS aligned controls, with regular independent audits and penetration tests.

Financial crime

KYC/KYB onboarding, sanctions and watchlist screening, and ongoing transaction monitoring.

We handle personal data in line with applicable data-protection laws, honor data-subject requests, and limit collection to what is necessary to operate accounts and meet regulatory obligations.

9 Threat detection & incident response

We monitor our environment continuously and maintain a documented incident-response plan that is tested periodically.

- Real-time monitoring and alerting across applications, infrastructure and money movement.
- Defined severity levels, on-call rotations and escalation paths.
- Post-incident reviews focused on root cause and prevention, with customer notification where required by law.

10 Third-party & vendor risk

Partners and vendors that touch customer data or funds are assessed before onboarding and reviewed on an ongoing basis. We prefer providers that hold their own recognized certifications and contractually require appropriate security and privacy commitments.

11 Business continuity & resilience

- Redundant, highly available infrastructure across multiple availability zones.
- Automated, encrypted backups with tested restore procedures.
- Documented business-continuity and disaster-recovery plans reviewed regularly.

12 Responsible disclosure

We welcome reports from the security community. If you believe you have found a vulnerability, please contact security@hitchpay.io. We investigate every report, work in good faith with researchers, and do not pursue legal action for good-faith testing that respects our users and data.

HitchPay Technologies, Inc. · 30 N Gould St, Sheridan, WY 82801 · security@hitchpay.io

HitchPay is a financial technology company, not a bank. Banking services are provided by Lead Bank, Member FDIC. This document is provided for informational purposes and does not create any contractual commitment.