



Security Statement

VERSION 1.0 · EFFECTIVE FROM 1 SEPTEMBER 2026 · LAST REVIEWED 24 JULY 2026

This statement summarises the technical and organisational measures we use to protect the CashXChain platform and the data on it. It is a public summary; it does not disclose internal procedures.

1. Our approach. Security is built into how we design, build and run the platform. We apply measures appropriate to the risk, in line with Article 32 [GDPR](#) ⁷, and review them regularly.

2. Encryption. All traffic to and from our platform is encrypted in transit using TLS 1.3, terminated at Cloudflare's edge. Data at rest is encrypted using AES-256.

3. Authentication and access. We protect accounts with multi-factor authentication, including support for passkeys (WebAuthn), and optional sign-in through established identity providers. Authentication is handled by our self-hosted authentication service. Internal access to systems and data uses role-based access control, enforces multi-factor authentication on all internal systems, follows the principle of least privilege, and is recorded through audit logging.

4. Network and infrastructure security. Our platform operates behind Cloudflare, which provides TLS, a web application firewall, DDoS protection, bot management and a privacy-preserving challenge (Turnstile). The platform is hosted with Amazon Web Services in the eu-central-1 (Frankfurt) region.

5. Secure development. We follow secure development practices, including code review and dependency management. An independent security design review was conducted by Certora in Q2 2026, covering the Rust/Axum backend architecture and blockchain integration.

6. Monitoring and incident response. We monitor our systems for security and availability. How and when we notify customers and authorities of security incidents and personal data breaches is set out in our [Incident Notification Policy](#). Security researchers can report issues through our [Responsible Disclosure](#) page.

7. Data protection. How we process personal data, including retention and your rights, is set out in our [Privacy Policy](#).

8. Resilience and backups. We take daily automated backups with 30-day retention, maintain point-in-time recovery for critical databases, and use cross-region replication for production data, so that we can restore availability and access in a timely way after an incident.

9. Certifications and roadmap. ISO 27001 certification and SOC 2 attestation are in active preparation as part of a dual-track implementation programme. Certification and attestation timelines will be published as they are confirmed.

10. Contact. Security questions can be sent to security@cashxchain.com; to report a vulnerability, see our Responsible Disclosure page.