

Security Posture Overview

Comprehensive Protection for Our Clients

Date: March 2026

Your Donors' Payment Information Never Touches Our Systems

When a donor enters their credit card details on your fundraising page, that information is captured directly by our PCI-certified payment partners through secure, isolated payment fields embedded on the page. The card data travels straight from the donor's browser to the payment processor – it never passes through or resides on Raisin's servers.

This is by design. Raisin does not store, process, or transmit credit card numbers or sensitive payment data in any form. We work exclusively with tokenized references, and only the last four digits of a card number are kept for donor identification. This means there is no payment card data on our systems that could be exposed in the event of a breach.

Independently Certified to the Highest Standard

In March 2026, Raisin completed a **PCI DSS v4.0.1 Level 1 Service Provider** assessment – the most rigorous tier of security certification available under the global Payment Card Industry Data Security Standard. An independent Qualified Security Assessor (**Control Gap Inc.**) spent a week on-site examining our security controls, interviewing staff, and testing our systems. They confirmed we meet all applicable requirements and issued both a **Report on Compliance** and **Attestation of Compliance**. This is the same level of certification held by major payment processors and global financial institutions.

The PCI DSS assessment validates our security controls across areas including network protection, access controls, encryption, vulnerability management, security monitoring, and incident response. All of these were independently confirmed to be operating effectively.

Beyond Payment Security

PCI DSS focuses on payment data protection. You also need to know that the platform will be available when you need it, that your data is processed accurately, and that donor privacy is respected. Here is how Raisin addresses each of these areas.

Platform Availability

Raisin's infrastructure is built for resilience. Our systems run across multiple independent data centre zones on Amazon Web Services, with automatic failover so that if one zone experiences a problem, traffic is redirected seamlessly. We maintain a formal Disaster Recovery Plan with defined recovery targets – in a typical zone failure, the platform recovers in approximately 20 minutes with no data loss. Backups are encrypted and replicated daily to a separate geographic region. Real-time monitoring alerts our team to any health issues immediately.

We also maintain a Business Continuity Policy that covers extreme scenarios – leadership succession, significant workforce disruption, and geographic disasters – so that operations continue regardless of circumstances.

Data Processing Integrity

Every change to the Raisin platform goes through a formal review and approval process before it reaches your live environment. Code changes are automatically scanned for security issues, and three independent reviewers must approve every change. A Change Control Board oversees all production changes with documented rollback plans in case anything needs to be reversed.

Test data is strictly separated from live data. The platform automatically removes all test information when an event goes live, and we conduct quarterly audits to verify this. All ten of our payment gateway partners – including Stripe, Moneris, PayPal, and Adyen – hold their own current PCI certifications, ensuring transaction processing is validated at every layer.

Privacy and Confidentiality

Raisin classifies all information by sensitivity level, with corresponding rules for how each category must be stored, transmitted, and eventually destroyed. When a client requests removal of constituent data, we follow a tracked procedure that ensures deletion across every system where that data exists – our database, backups, content delivery network, and all internal communication channels.

Personal and sensitive data is never used in testing or development environments. All data is encrypted both in transit and at rest. Employees access data strictly on a need-to-know basis, with regular access reviews, mandatory background checks, and signed confidentiality agreements. Our AI Usage Policy explicitly prohibits sharing any client or donor data with external AI tools.

Our Commitment to You

We take seriously the trust your donors place in your organization, and the trust you place in us. Our security program reflects that commitment through independent certification, continuous monitoring by a dedicated managed security partner, quarterly vulnerability testing, annual penetration testing, and a trained incident response team ready to act at any time. Every employee undergoes background checks and annual security training.

We partner with recognized industry leaders at every layer – AWS for cloud infrastructure, Sophos for endpoint protection, CyberHunter for 24/7 managed security services, and ten PCI-certified payment processors. Each maintains their own independent security certifications, so your donors' information is protected at every step.

You can be confident that Raisin provides a secure, reliable, and independently validated platform for your organization's fundraising needs.

© 2026 A.K.A. New Media Inc. (Raisin Software).