



Fundraise Up security measures for nonprofits

Best-in-class security standards
for donor and organizational safety

Table of contents

[How we secure your donors' data →](#)

[How we secure your donors' payments →](#)

[How we secure your team's data →](#)

[How we help you be compliant →](#)

[How we stay on top of your security →](#)

At Fundraise Up, we're serious about keeping your fundraising secure. That's why we're always ahead of the curve when it comes to protecting your campaigns from any threats. With the best encryption technologies, strict compliance with payment standards, and advanced anti-fraud tactics, we create a safe space where your donor and organization data are thoroughly protected.

In this guide, you'll find a clear breakdown of all the security steps we take to make sure every transaction and piece of data is handled safely. We cover everything from securing donor payments to protecting sensitive information and making sure your team works in a secure environment. Our goal is to handle the security so you can focus on your mission, knowing everything is under control.

How we secure your donors' data

Protecting the privacy and integrity of your donors' data is crucial. We implement comprehensive data security measures to ensure that all personal information is handled responsibly:

Data privacy

We maintain transparency in our data handling practices. Our detailed Information Security and Data Protection policies are readily accessible and explain how we store, transmit, and protect personal information. Moreover, find more info in our handy [FAQ](#).

Data deletion and retention

We strictly manage data retention and deletion protocols to comply with legal obligations and ensure that information is not kept longer than necessary. Secure deletion practices are employed to protect against unauthorized access or breaches.

Backup and recovery

We implement stringent backup and recovery procedures to ensure data integrity and availability. Bank-level data protections provide 99.9% uptime year-round and ensure platform redundancy so that your account is always online and your data is secured. We ensure that backups are performed at least daily and are retained for a year, to meet both operational needs and compliance requirements.

SSL requirements

A valid SSL certificate is mandatory for all client sites using our platform to ensure secure, encrypted connections. This is a critical component of our security framework to protect data integrity and privacy.

How we secure your donors' payments

Anti-fraud measures

Fraudulent activities can undermine donor confidence and disrupt your fundraising efforts. That's why we have developed our own extensive anti-fraud technological solution, adding an additional layer of protection for nonprofits.

By implementing these comprehensive anti-fraud measures, Fundraise Up ensures that donations are legitimate, minimizes the risk of chargebacks and financial losses, and maintains compliance with legal and financial regulations.

We use a combination of advanced machine learning algorithms and human oversight to detect and effectively prevent fraud.

Our strategies include:

- **Proxy detection:** Our advanced fraud protection tools flag transactions for review by our fraud prevention team when someone uses a proxy to make a donation on your website.
- **HoneyPot:** This approach discreetly manages and monitors fraudulent activities without alerting fraudsters by simulating a card issue instead of banning it.
- **Country flagging:** Some countries have high fraud rates - when a transaction originates from one of these countries, we flag it for review by our team.
- **Proprietary AI:** We use a propriety fraud detection AI that analyzes device characteristics and activity indicators for millions of transactions to signal and neutralize fraud before it occurs.
- **Behavior analysis:** Using machine learning, we detect suspicious behavior based on website traffic and transactional data patterns.
- **Human review:** If a transaction fails or is flagged for fraud, someone from Fundraise Up's fraud prevention team reviews the transaction to determine whether it should be processed or blocked.

Moreover, we provide transparency into the effectiveness of these measures by displaying prevented fraud incidents within your Insights Dashboard.

Learn more about [Fraud protection](#)

Performance

See how your campaigns are performing, and how Fundraise Up is boosting your efforts.

Saved recurring plans

Prevented the cancellation of a total of

546 plans

Pre-donation upsell [?]

Boosted your revenue from one-time donations by an extra

+ \$6,800.00/year

Post-donation upsell [?]

Boosted your revenue from one-time donations by an extra

+ \$2,500.00/year

Covered costs

You're getting more supporters to cover transaction costs with the AI

AI Adaptive

Fraud prevented

Fraudulent donations that were detected and prevented

12 payments

Mobile users [?]

Percentage of donations made on a mobile device

50%

PCI DSS Level 1

We adhere to the highest standards of payment security, maintaining PCI DSS Level 1 compliance. It's important to note that while we facilitate secure transactions, the direct processing is handled by our PCI-compliant partners, such as Stripe.

Tokenized payments

Fundraise Up processes transactions directly through Stripe as tokenized payments, ensuring that sensitive payment details are never exposed.

How we secure your team's data

Effective management of roles and permissions is essential for maintaining security within your tech environment. At Fundraise Up, we provide robust tools to control access and protect sensitive information.

Admin control over roles and permissions

With Fundraise Up, you have the ability to assign and customize roles and permissions tailored to the specific needs of your team.

- **Customizable access**

Administrators can define access levels so team members only have the necessary permissions to perform their roles without compromising data security.

- **Segmented user roles**

We offer predefined roles such as Organization Administrators, Campaign Administrators, and Support Specialists, each with tailored access to suit different responsibilities and data sensitivity levels.

For more detailed information on setting up and managing roles, please visit our comprehensive guide [here](#).

How we help you be compliant

Navigating the complexities of regulatory compliance is a significant challenge for nonprofits. Fundraise Up is committed to helping you meet these challenges by maintaining the highest standards and facilitating compliance through our platform's design.

Compliance certificates and standards

Our platform holds several key certifications, making our solution a leader in the industry by providing top-level security:



- **PCI DSS**

Ensures the secure handling of credit card information by our system and our partners.

- **ISO 27001**

Confirms our comprehensive approach to managing information security risks across all organizational levels.

- **SOC 2**

Demonstrates that our data management practices adhere to strict industry standards for security, availability, processing integrity, confidentiality, and privacy.

- **WCAG 2.1 AA**

Ensures that our web platforms are accessible to all users, including those with disabilities, meeting international web accessibility standards.

- **GDPR**

Guarantees compliance with the General Data Protection Regulation, safeguarding data protection and privacy for individuals within the European Union and the European Economic Area.

How we stay on top of your security

At Fundraise Up, continual improvement is part of our security ethos. We employ various measures to stay ahead of potential threats and ensure that our systems and your data remain secure.

Team member management and training

- **Regular Training:** All team members undergo regular security training to stay updated on the latest security.
- **Background Checks:** We conduct thorough background checks on all employees, especially those handling sensitive data, to maintain a trustworthy team.
- **Role-Specific Training:** Specific training programs are tailored to the needs and access privileges of different roles within our organization, ensuring that every team member is well-prepared to handle their responsibilities securely.

Incident response

We have a comprehensive incident response plan in place to swiftly manage and mitigate any security breaches. This plan is regularly reviewed and updated to adapt to new security challenges.

Transparency is key to trust and operational integrity. We maintain a dedicated [Status page](#) that provides real-time updates on our platform's state. This page is an essential resource for our clients to stay informed about the operational status of Fundraise Up.

Regular security assessments

We conduct annual penetration tests and regular security assessments to identify and rectify vulnerabilities.