WHITEPAPER

Security at Chariot

Welcome to Chariot - Where security comes first

Welcome to Chariot - We're serious about safeguarding data.

Chariot is a payment network for Donor Advised Funds. We build the financial infrastructure that connects these complex charitable assets to nonprofits. Donor Advised Funds hold more than $234B in philanthropic dollars and are considered the fastest-growing vehicle in philanthropy. Today, there are nearly 1.3M DAF accounts - a number that has increased more than 400% over the last five years. Despite this tremendous growth, DAFs remain unconnected to the broader online giving environment. Millions of DAF holders are stuck behind login portals to make a donation. Meanwhile, nonprofit organizations have no meaningful way of connecting directly with these donors.

The democratization and growth of the DAF market are driving providers to build and invest in the open financial infrastructure required for donors to easily and securely give with their DAF to the causes they care about most. With Chariot, nonprofits simply add our payment option to their donation form, enabling donors to 'one-click' give with their DAF. This whitepaper will help you understand the key elements of Chariot's security.

This whitepaper answers the following questions:

Chariot - The Trusted API

Since day one, security and transparency have always been priorities at Chariot. With Chariot's universal and reliable API, nonprofits can accept grant requests from Donor Advised Funds through a single API.

As always, we encourage you to contact us for more information. Contact us via email at contact@givechariot.com if you have any other questions.

Safeguarding Your Data

Protecting personal information is our top priority. For the sake of our donors, we don't compromise or cut corners when it comes to data security. As part of that commitment, we operate with the utmost transparency. The following overview provides a high-level look at our robust security practices at Chariot.

Security Principles

The following principles guide our approach to security.

Proactive security
We acknowledge that our security focus should be defined by the unique risks we face. Therefore, we continuously identify and manage emerging threats and significant risks.

Minimum-information
We aim to ensure users and systems have the minimum access necessary to perform their functions successfully.

Separation of knowledge
Each user or system has a limited amount of authority.

Levels of defense
Layered security mechanisms increase the security of the system as a whole.

Minimize surface area
Every feature adds a certain amount of risk to an application's overall security. We keep a robust security by minimizing points of entry.

Continuous logging and monitoring
We enforce continuous monitoring and logging mechanisms to detect unauthorized use and to support incident investigations.

Customer Data & Management

Chariot is built with control, security, and transparency.

Secure login that is never stored

- User credentials are passed through to each Donor Advised Fund provider and are never stored.
- We employe secure network connections (HTTPS/TLS), so your credentials are always encrypted in transit.
- When submitting grant requests on your behalf, we utilize secure and reliable APIs.
- Multi-factor authentication with participating providers adds an extra layer of security.

Always private

- Your Donor Advised Fund data belongs to you. We build the tools to make giving your charitable dollars simple and secure.
- Chariot never submits grants without donor consent and verification.
- Chariot will never be able to access your personal data.
- Nonprofits (or any other third party) will never be able to access your personal data.

Encryption & Network Security

Chariot utilizes encryption, limited access, and other industry best practices to protect your data

Chariot is committed to protecting data and privacy.
That's why we use industry-vetted, trusted protocols and standards. Our infrastructure is designed to follow industry standards to keep your data safe.

We establish strong defenses at points of entry.
We use a combination of the Transport Layer Security (TLS) and Advanced Encryption Standard (AES-256) to keep your personal information safe.

We take all necessary infrastructure precautions.
All of our services run in Amazon Web Services (AWS). We don't host or run our own routers, load balancers, DNS servers, or physical servers. AWS regularly undergoes independent verification of security, privacy, and compliance controls against the following standards: ISO/IEC 27001, ISO/IEC 27017, SOC 1, SOC 2, SOC 3, PCI DSS, HIPAA, CSA Star, FedRAMP, and many others. You can read more about their practices here.

Infrastructure Security

Our infrastructure is designed to follow industry standards to keep your data and your customers' data safe

Secure cloud infrastructure

Chariot is hosted on AWS cloud infrastructure, leveraging years of safety enhancements to ensure maximum performance, resilience, and speed of deployment.

- Network segregation—our infrastructure implements a tiered network architecture to isolate web servers and data stores from direct internet connectivity.
- DDoS prevention—AWS Shield Standard defends against network and transport layer DDoS attacks that target your website or applications.
- Intrusion detection—our intrusion detection systems (AWS GuardDuty) continuously monitor our infrastructure and workloads for malicious activity and deliver detailed security findings for visibility and remediation.
- Audit trail—we record all event history of our AWS account activity to enable security analysis, resource change tracking, troubleshooting, and detecting unusual activity

Logging and monitoring

By keeping a watchful eye over the production environment and maintaining detailed logs, we can identify problems—and implement solutions—extremely quickly. We log all impactful changes, actions, and authentication attempts, and maintain an audit trail accessible to authorized employees.

Access to the production environment

Only authorized personnel can access the Chariot production environment, which is principally hosted on AWS.

Patching

Chariot addresses vulnerabilities through security updates and patches provided by vendors. If we cannot perform a live patch, we use the most recently available base image and cycle assets to enable updates.

Asset management

Every cloud asset that is a part of our infrastructure is inventoried and documented to ensure that it is secured appropriately.

Proactive Security

As part of our proactive approach to security, Chariot takes several steps to recognize potential threats, mitigate them, and respond swiftly to incidents.

Our security measures are ever-evolving to keep pace with the changing threat landscape.

Our work on security and privacy efforts does not have an end; it's a continuous cycle of researching, revising, implementing, testing, fixing, scaling, and blocking. We are constantly working to meet and exceed what is asked of us from regulators, investors, partners, and users, and we collectively live the security processes daily. Security and privacy are integral to our culture.

Looking Ahead

Chariot is committed to staying at the forefront of security, from earning additional certifications to following future leading practices such as tokenization. Our highly informed leadership team will continue to stay up-to-date regarding the latest developments in security, so we can continue to serve as a highly trusted partner.

Learn More

To get more information about our comprehensive, multi-layer approach to security, please reach out to us via email at contact@givechariot.com, or visit givechariot.com.