At Bloomerang, we know that your donors trust you with their personal information. The following multi-layered security policy explains why you can feel safe with Bloomerang.

Hosting Environment

All of our servers are hosted by Amazon Web Services (AWS) in their secure cloud environment. AWS provides a solid foundation of security and a set of tools we use to ensure your data's security.

Data Transmission

All data transmitted between your browser or your donor's browser and Bloomerang is secured via HTTPS. This ensures two things:

1. Authentication: when you're using Bloomerang, you can be sure that it's actually Bloomerang and not a third party pretending to be Bloomerang
2. Encryption: all messages sent to and from Bloomerang are encrypted using a secure encryption method, TLS. Bloomerang specifically does not support SSL, which has been shown to no longer be secure.

Firewalls

The Bloomerang servers live in an AWS Virtual Private Cloud (VPC). AWS ensures that all traffic between servers in the VPC is private. We use security groups which limit what kind of traffic is allowed into the VPC and from where. For example, everyone has access to reach the Bloomerang web servers on port 443 (HTTPS) to use the application, but bastion servers can only be logged into from Bloomerang headquarters and a select few of our DevOps team's residences. In addition, traffic within the VPC and outbound from the VPC is also restricted via security groups.

Data Storage

Bloomerang database servers are encrypted at rest.

Configuration Auditing

Bloomerang uses AWS Config, AWS CloudTrail, and AWS Inspector to audit and monitor our AWS configuration. This ensures that Bloomerang follows AWS's security best practices.

Backups

We use Amazon RDS automated backups to take a snapshot of our database servers every night. These backups are retained for seven days for disaster recovery in case we would ever need to restore the entire system.

Additionally, we take individual database backups so that we can quickly restore a single organization's database. These are stored in Amazon's secure cloud file storage service, S3. We retain daily backups for 30 days, weekly backups for 90 days, and monthly backups indefinitely.

Secure Servers

We deploy OS security patches monthly or more frequently as needed.

Secure Application

All Bloomerang code is reviewed by a senior software engineer for security concerns.

Data Access

Only Bloomerang engineers who perform data services have access to the Bloomerang database directly.

Physical Access

AWS ensures physical and operational security of the Bloomerang server environment. See this whitepaper for more information.

Password Policy

Bloomerang requires use of an 8 or more character password, although we recommend that you use at least 12 characters. We also recommend that you use a unique password for Bloomerang that you do not use anywhere else.

We allow five failed login attempts before we lock out a user account. The lockout expires after five minutes.

Password reset emails may be generated by a user or by your account administrator.

Passwords are hashed using SHA-512 and a random 6-character salt for database storage. We do not store your password in our database.

Credit Card Security

Stripe

For customers who use Stripe as their payment processor, Bloomerang uses Stripe Elements in online forms to collect credit card information and submit it to Stripe. Using Stripe Elements minimizes your PCI scope, because the credit card fields are hosted within an iframe by Stripe and not by your web site. With Stripe Elements, the credit card number and CVV are transmitted

directly from a donor's browser to Stripe. Protected credit card information (the full credit card number and CVV) is never sent to your website or to Bloomerang. Stripe is a Level 1 PCI Compliant vendor.

Spreedly

For customers who use other payment processors, Bloomerang uses Spreedly Express in online forms to collect credit card information and submit it to your processor. Using Spreedly Express minimizes your PCI scope, because the credit card fields are hosted within an iframe by Spreedly and not by your web site. With Spreedly Express, the credit card number and CVV are transmitted directly from a donor's browser to Spreedly and then to your credit card processor. Protected credit card information (the full credit card number and CVV) is never sent to your website or to Bloomerang. Spreedly is a Level 1 PCI Compliant vendor.