Blackbaud Client Data Policy

Blackbaud staff will request access to your organization's data or database only when necessary to assist your organization with data conversion or software issues. Data is defined as not only a database, but also any files (i.e. .rpt, .mdb, .mdf, etc.), screen shots or hard copies of reports, statements, etc. Our database access, security criteria, database usage, user review, data library and confidentiality policies are further explained below.

Database Access:

You effectually grant Blackbaud access to your data only by sending a copy of your database, providing Blackbaud with a database login for software as a service (SaaS) or web-based products, or via remote access (WebEx, VPN, screen share, etc.) when applicable. You may send data using one of the following methods:

- Upload a password-protected zipped copy of your database via File Transfer Protocol (FTP) to our secured website.
- Send a copy of your database via US Mail, FedEx, UPS, etc. (mostly larger CRM dBs) via an encrypted external storage device

We will not request your personal login. However, if a test login is needed for database testing, it will be **your responsibility** to change it following the completion of our work.

When accessing your data on premise at Blackbaud, data is obfuscated as it is restored, assuring sensitive data is not consumable in its raw format.

Security Criteria:

When providing a login for Blackbaud staff to access your database and environment, ensure it meets the following criteria:

User name:

- Must reference a particular user; generic user names are not permitted*
- User name must *start* with BBSUPP
- Must be between 7 and 20 characters

Password:

- Cannot contain all or part of the user name
- Must be at least 8 characters in length
- Must contain characters from three of the four following categories (no hyphens):
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (e.g. $, #, %)

Username and password must be communicated to Blackbaud via a phone call. Blackbaud will store user name and passwords in an encrypted tool only, not in Clarify case notes or any other publicly accessible location, and will not share them with peers in Support or any other department. If necessary for another Blackbaud employee to access the data, a new user name and password must be provided..

***** Only specific user names may be used by Blackbaud staff to access your environment and database. For auditing and data security practices, we cannot use a generic login (e.g., "Blackbaud1"), even upon your organization's request.

Database Usage:

Due to the size and complexity of certain Blackbaud software, we may need direct access to your organization's database to view configuration and customizations unique to your environment when troubleshooting software issues. Access to your Production database is a last resort; we will first follow common troubleshooting steps to duplicate the issue, including:

1. Testing in a sample database
2. Conducting screen-sharing sessions to observe the issue in your environment
3. Testing in a staging or development environment

When troubleshooting an issue in your live data, we will limit testing to read-only processes (e.g., queries). Occasionally, we may need to perform tests that will affect your data (e.g., adding a test record). As these situations arise, we may work with a user at your organization who can conduct tasks in a staging or test environment, if available. If changes to your live environment are necessary, we **highly recommend** that you ensure appropriate backups are made.

User Review Process:

For SaaS or web-based products, we recommend that you regularly review which individuals have been granted access to your database. Periodic reviews may also be requested with Blackbaud management (or your technical account manager, if applicable) to ensure access to users is current and corresponds with expected Blackbaud staff. Database access for your organization's end users is managed solely through your organization's Help Desk.

Data Library & Confidentiality Policy:

We are committed to the privacy, security and confidentiality of the information within each organization's database, including the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and state law, whenever applicable. With the exception of data that is stored within SaaS or web-based products, we keep copies of client databases on our secured data library server. Data is stored for a 90 day period on this secured directory in a folder designated with the client's unique site ID, or longer if requested by the Client. All other copies of client data are deleted or overwritten after use. We will also shred all reports, statements and forms, and securely destroy electronic protected health information and other personal information subject to secure destruction requirements

Regulations and Laws:

Blackbaud stays abreast of current government regulations whenever possible, including but not limited to:

- HIPAA
- PA-DSS
- PCI
- PIPEDA
- Grateful Patient, HIPAA and PHI