

Getting Started

WITH CUSTOMER SUCCESS



Your Commitment to Security

We're committed to championing your organization's security. However, this dedication to security is a partnership – and with all partnerships, we ask that your team also makes a commitment to keeping your data secure. Here are some tips to ensure your data is secure.



Determine and Restrict Access Rights

Each of your team members may need specific levels of access to do their job. Be sure that access rights and permissions correspond to their role, and do not allow users or departments to have a shared set of credentials. Your organization determines who should have user and administrator rights and, for your security, these rights must be assigned by your organization.



Develop a Security Plan

A security plan is a set of procedures and policies that govern how data is handled in your organization. The plan should outline well-defined and clear practices to ensure that your data stays secure.



Enable Single Sign-on or Encourage Multi-Factor Authentication

[Blackbaud ID Single Sign-On](#) allows administrators to manage authentication for users signing in with email addresses on their organization domain. While your email address and password help secure your Blackbaud ID, you can increase security with [multi-factor authentication](#). Multi-factor authentication enables your Blackbaud ID to require a unique verification code — received on your personal device — in addition to your email address and password.



Require Strong Passwords

While Blackbaud's website and solutions have strong password requirements, be sure to encourage users and administrators to be thoughtful about their password complexity.



Train Your Staff

Each member of your team should receive the training that applies to their role. Blackbaud University offers eLearning and instructor-led courses that can be tailored to fit the level of learning that fits each user and administrator.



Implement Policies

As you create a security plan and other procedures for your organization, be sure these are strictly applied. Integrate these into new employee/user orientation to be sure everyone on your team is well-informed and able to implement the policies in their day-to-day role.