Blackbaud Cyber Security Overview
Our Information Security team leverages the industry standard CIA Triad Model (Confidentiality, Integrity, Availability) in conjunction with various industry control frameworks, such as the NIST CSF, PCI DSS, ISO27001, SOC 1, SOC 1 type 2, and others to protect our solutions.

**CONFIDENTIALITY**
Information is not disclosed to unauthorized individuals

**INTEGRITY**
Ensuring accuracy and completeness of data that can’t be modified in any unauthorized manners

**AVAILABILITY**
Information should be readily available to authorized users whenever it is needed

This white paper is for informational purposes only. Blackbaud makes no representations or warranties, expressed or implied, in this summary. The information contained in this document represents the current view of Blackbaud, Inc., on the items discussed as of the date of this publication.

All Blackbaud product names appearing herein are trademarks or registered trademarks of Blackbaud, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Transparency

Blackbaud provides audit reports by request to our subscription customers, their auditors, and our prospective customers, including SOC 2 type 2, SOC 1 type 1, and bridge letters for both SOC 1 and 2 reports, where applicable*.

Blackbaud provides PA-DSS and PCI-DSS attestations of compliance to Blackbaud Internet Services and Blackbaud Payment Solutions*.

Blackbaud also leverages the Cloud Security Alliance's CAIQ-Lite assessment questionnaires to provide transparency regarding the adherence of our products to the CSA Cloud Controls Matrix. These assessments are made available via the Cloud Security Alliance.*

Security

INFRASTRUCTURE SECURITY

Our world-class security, privacy, and risk-management teams work every day to ensure the safety of your data by adhering to industry standard practices, conducting ongoing risk assessments, aggressively testing the security of our products, and continually assessing our infrastructure.

As such, our promise to you is that your Blackbaud solution is always secure, protected, and reliable through:

• Robust and continuous Cloud Account/Subscription Governance and control monitoring
• Clear security requirements and reporting on data protection, encryption, and monitoring
• Routine vulnerability assessments and DDoS automitigation response
• Active participation in CyberSecurity thought leadership:
  • Blackbaud is a member of Cloud Security Alliance (CSA) and assesses our products and environments against the CSA CAIQ (consensus Assessment Initiative Questionnaire).
  • Blackbaud Security is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), a thought leadership and information sharing community for collaboration on critical security threats facing the global financial services sector.
  • Blackbaud partners with the Information Sharing and Analysis Center for Nongovernmental Organizations (NGO-ISAC) to participate in collaboration regarding US-Based nonprofit/nongovernmental organizations under attack from sophisticated threat actors.
  • Partnership with Microsoft and Azure
    • Blackbaud engages in an Azure-first model and partners consistently with Microsoft. This provides us access to industry threat intelligence and early previews regarding upcoming Azure feature capabilities and security releases.
  • Partnerships with other cloud providers and independent third parties for reviews

Blackbaud also leverages tactical Cyber Security strategies for safeguarding our environments and data by utilizing the NSA’s Defense in Depth techniques and layered security, including:

• Data Protection
• Application Security
• Host Based Security
• Internal Network Security Measures
• Perimeter Security
• Physical Security
• Policies/Procedures/Awareness
• Blackbaud’s Cloud Security includes rigorous standards across physical, application, and personnel security

Blackbaud utilizes System Center (SCOM) for internal out of the box monitoring with customized management packs that monitor within the application layer from the inside out to include an early warning detection system that allow us the time to investigate and respond to an issue before it becomes an impactful event.

*compliance certifications and assessments may vary by product
PHYSICAL SECURITY
Blackbaud enforces strict physical datacenter security based on best practices and SSAE18 audit guidelines:

- All building entrances, the datacenter floor, and secure areas require card key access. The datacenter floor and secure areas also require two factor biometric authentication (hand/finger prints and iris scan).
- Active patrol guards are onsite to monitor the interior and exterior of our facilities 24 hours a day, 365 days a year. We also have security cameras covering all entrances, alternate workspaces, and the datacenter floor.

APPLICATION SECURITY
Blackbaud ensures the security of our applications through:

- Constant education and partnership with Blackbaud development community with robust and varied training programs
- Routine vulnerability assessments
- Continually empowering our developers with security tools to leverage early in the security SDLC processes

DATA PROTECTION
Blackbaud ensures the sanctity of our and our customers’ data applications through:

- Encryption
  - Blackbaud uses various strong encryption mechanisms across our environments and products, including TLS 1.2, AES 256, RSA 1024, and other FIPS140-2 encryption algorithms.
- Authentication
  - Through Blackbaud ID, we support multi-factor authentication and modern identity providers (IdP) such as Microsoft Azure Active Directory, Okta, and SAML-based providers such as Google G-Suite so you can control your end-user login experience*.

SECURITY AWARENESS
Blackbaud employees are all engaged in on-going Security Awareness and rigorous training campaigns to ensure they are empowered to protect both Blackbaud’s and our customers’ data. All employees are provided continual phishing simulation testing to increase their awareness of cyber security social engineering and phishing techniques.

The Blackbaud Security team additionally partakes in global communities and conference platforms—such as bbcon, WISCYS, and local security conferences—to share information and present on industry best practices to improve the community’s security awareness posture.

TESTING
The Blackbaud Security team prioritizes routine testing to identify and remediate vulnerabilities and risks by leveraging:

- Dedicated Red Team
- Routine Penetration Testing
- Routine Code and Vulnerability Scanning
- Cloud Audits & Assessments
- Phishing Simulations

Privacy
Driving social good on a global scale—spanning the public, private, and social sectors—requires a detailed understanding of privacy standards. Blackbaud has dedicated legal counsel who continually evaluate upcoming and changing regulations as they relate to data privacy to ensure we are aligned to these regulations, as well as providing thought leadership for our customers on the operational impact of these regulations and compliance requirements.

*compliance certifications may vary by product
Blackbaud is committed to providing products and services that enable customers to comply with the privacy laws applicable to them. We tirelessly track and interpret pending legislation to ensure that Blackbaud provides the features you need to protect the privacy of your constituents while managing data in a compliant way. As privacy legislation evolves, our products do too. Further, we will continue to work on ways to improve the user experience in the products, specifically as regards the capture, recording, and use of your supporters’ consent. We ensure that (when applicable) our products and internal processes comply with and enable customers to comply with:

- General Data Protection Regulation (GDPR): A European Union regulation that establishes commercial standards for data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA)
  - Learn more about Blackbaud’s GDPR compliance
  - Blackbaud has also developed a GDPR Toolkit, with specific recommendations per product to help enable our customers to ensure they are compliant with GDPR
  - Blackbaud GDPR Product Documentation

- Health Insurance Portability and Accountability Act (HIPAA): A U.S. law that provides data privacy and security provisions for safeguarding Protected Health Information (PHI)
  - Blackbaud regularly performs assessments for our compliance with industry-standard data protection protocols such as HIPAA.
  - All Blackbaud products available to customers in the healthcare sector are assessed for compliance with HIPAA annually. Additionally, these products are also reviewed to ensure customers can achieve and maintain their own HIPAA compliance obligations when performing fundraising and data management activities using Blackbaud solutions.
  - California Consumer Privacy Act (CCPA): a U.S. bill that enhances privacy rights and consumer protection for residents of California.

- As of the effective date of the California Consumer Privacy Act (CCPA), Blackbaud will be fully compliant with this law.
- Similar to the guidance provided on GDPR, prior to the effective date of the CCPA, Blackbaud will issue guidance on how our various solutions can be used for our customers to help them comply with these regulations
- Global email laws, including CAN-SPAM, CASL, and PECR: Laws such as CAN-SPAM in the US, Canada’s Anti-Spam Legislation, and the UK’s Privacy and Electronic Communications Regulations govern the sending of electronic marketing messages.
  - Blackbaud solutions contain functionality enabling customers to collect, record, and use explicit consent to receive marketing emails in accordance with email laws.
  - Our email solutions allow customers to send email in line with legal requirements and best practices, such as unsubscribe functionality.

We understand regulatory requirements and constituent expectations around data privacy are a key priority for our customers as well. For more information about safeguarding your constituent data, reference the Blackbaud Institute’s Privacy Toolkit.

Reliability
Blackbaud designs mission-critical cloud solutions exclusively for social good organizations.

Our commitment to reliability is backed by our industry-leading service level agreement of 99.9% availability—or you will be eligible for credits to your subscription.

Our cloud solutions are modern and innovative and allow your teams to be productive on any device at any time by leveraging Blackbaud SKY UX for natively mobile experiences.

We amplify continuity of service through extensive disaster recovery policies, regular offsite backups (performed nightly, weekly, or monthly), and redundant architecture.