Blackbaud and the Public Cloud

Foreward

As the leading provider of software for powering social impact, Blackbaud never stops working to earn and keep your trust. No other partner combines cloud innovation with our deep understanding of the unique needs of purpose-led organizations. Nonprofits, foundations, education institutions, healthcare organizations, faith communities, arts and cultural organizations, and companies need the performance, security, and ease of the public cloud.

We accelerate the impact of anyone dedicated to purpose driven work through essential software that drives outcomes for our customers. Our cloud solutions provide modern architecture that advances ease-of-use, enables rapid innovation and scales to meet customer needs. Blackbaud's solutions allow you the flexibility to extend and expand within your organization, all with security and reliability.

Our relationships with industry-leading Cloud Service Providers (CSPs) are an extension of Blackbaud's commitment to our customers. We partner with CSPs to ensure your solutions benefit from industry-standard infrastructure now and into the future. The public cloud leverages security, reliability, and performance.

Key benefits of Blackbaud's Cloud Operations include:

- Innovative, modern cloud infrastructure and a commitment to 99.9% uptime and availability—monitored around the clock, 365 days per year—so your applications are available when you need them
- An industry-leading investment in research and development,
- Adherence to the highest-level compliance certifications and laws, including PCI-DSS, PCI PA-DSS, SSAE 18 (SOC1, SOC2), GDPR, and alignment to best practices according to the Cloud Security Alliance and others

Blackbaud's Preferred Cloud Service Provider

In addition to our internal enterprise cybersecurity experts, we partner with a global corps of external experts to supplement our team. With Blackbaud and Microsoft Azure, our preferred Cloud Service Provider (CSP), you will benefit from the expertise of a global team of security and privacy leaders and practitioners.

Microsoft Azure is an ever-expanding set of cloud services that helps organizations meet their business challenges. These services provide the freedom to build, manage, and deploy applications on a massive, global network. Gartner has positioned Microsoft Azure as a leader in 18 different Gartner Magic Quadrant categories, and it has received numerous industry accolades for security and scale.

Microsoft Azure infrastructure is designed and managed in accordance with a variety of IT security standards. Blackbaud's relationship with Microsoft Azure as our preferred CSP provides access to industry-leading threat intelligence and early previews regarding upcoming Azure features, capabilities, and security releases.

PHYSICAL SECURITY

Blackbaud provides a hosting environment that aligns with strict physical security measures based on best practices and SSAE18 audit guidelines. No matter the provider, our cloud software portfolio meets robust physical security standards. Blackbaud's CSPs take a layered approach to physical security to reduce the risk of unauthorized users gaining physical access to data.

Microsoft Azure's hosting environment offers extensive protection layers and provides the following:

- Access must be requested prior to arriving at the hosting facility, and a valid business justification must be provided for each visit. All requests are approved on a need-to-access basis by Microsoft employees.
- The Azure physical perimeter contains tall fences made of steel and concrete.
- Active patrol guards are onsite to monitor and patrol the interior and exterior of our hosting facilities 24 hours a day, 365 days a year with security cameras covering all entrances, alternate workspaces, and the facility floor.
- All building entrances, the hosting facility floor, and secure areas require card key access.
- The facility floor and secure areas require two-factor biometric authentication (hand/fingerprints and iris scan) along with a full body metal detection screening. After Microsoft grants permission, access is granted to a discrete area of the facility before permission expires. Only approved devices are allowed in the facility.
- For additional information, please refer to the following Microsoft resource: Azure Facilities, Premises, and Physical Security and Azure Global Infrastructure.

RECOVERABILITY, RETENTION, & BACKUPS

We amplify continuity of service through extensive disaster recovery policies and regular offsite backups (performed hourly or upon each 5 megabyte data increase).

Blackbaud's CSPs help ensure that data is protected if there is a cyber attack or physical damage to a hosting facility via the following capabilities:

- Data can be replicated within a selected geographic area for redundancy and cannot be transmitted outside of the perimeter.
- Blackbaud uses a combination of the following replication options when storage accounts are created, which may differ based on customer product and hosting location:
  - Geo-redundant storage (GRS): Geo-redundant storage is enabled for storage accounts by default when they are created. GRS maintains six copies of data. With GRS, data is replicated three times within the primary region. Data is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, Azure Storage fails over to the secondary region. GRS helps ensure that your data is durable in two separate regions. For customers with geographical restrictions, GRS may not be available.
  - Locally redundant storage (LRS): Locally redundant storage maintains three copies of data. LRS is replicated three times within a single facility in

Continued on next page...

a single region. LRS protects data from normal hardware failures, but not from a failure of a single facility.

- Zone-redundant storage (ZRS): Zone-redundant storage maintains three copies of data. ZRS is replicated three times across two to three facilities to provide higher durability than LRS. Replication occurs within a single region or across two regions. ZRS helps ensure that data is durable within a single region. For customers with geographical restrictions, ZRS may not be available.
- Hosting facilities have native redundant power, networking, and cooling systems, as well as software elements like safe deployment processes, impact-less maintenance, and failure prediction enabled by machine learning.

DATA PROTECTION

Blackbaud's partnership with CSPs provides an additional layer of protection for our customers. With Microsoft Azure, for instance, we ensure the reliability and security of our customers' data applications through:

- Data Separation
  - We employ a highly segmented network topology to ensure that only necessary network traffic is allowed.
  - All changes made to the environment are deployed in two lower-level environments before they are moved into in production.
  - Human access is highly controlled and limited in scope and breadth.
- Encryption
  - All network traffic traverses the Internet via fully encrypted network protocols.
  - 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.
  - Blackbaud leverages native full disk encryption in the Azure environment with BitLocker that leverages the AES encryption algorithm with a 256-bit key and a sector-by-sector Chained Block Cipher (CBC). Keys are maintained in a secure vault.
  - The integrated protocol checksum ensures data integrity while the strength of the key generation and exchange algorithms ensure data confidentiality.
  - "Encryption by default" using MACsec (an IEEE standard at the data-link layer) is enabled for all Azure traffic to ensure confidentiality and integrity of customer data.
  - All Windows servers are running in Windows core mode with a minimal configuration to reduce attack surface.
  - Database backup encryption exists with separate unique keys per customer.
  - Read Only access utilizes IP AllowListing
  - Within the application itself, specific fields are encrypted at rest using AES 256. For additional information, refer to the following resources:
    - What fields are encrypted in my Blackbaud solution?
    - Azure Disk Encryption for Windows Virtual Machines
- Media Destruction
  - Blackbaud uses industry recommended secure media destruction techniques (NIST 800-88 guidelines for media sanitization) for the destruction of all media types. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that cannot be wiped, Microsoft uses a destruction process that renders the recovery of information impossible. Microsoft determines the means of disposal according to the asset type and retains records of the destruction.

Blackbaud leverages Azure's security and best practice recommendations. For more information, visit the Microsoft Trust Center and Microsoft Azure's compliance documentation.

Continued on next page...

Blackbaud's Global Trust and Security Program

In addition to partnerships with CSPs, Blackbaud's extensive Global Trust and Security Program is committed to providing confidence that your organization's technology and data are secure.

You can rest assured that we are working 24/7/365 with the goal of protecting you to ensure you and your data can confidently move forward in an ever-evolving threat landscape.

APPLICATION SECURITY

Blackbaud employs measures to protect our applications through:

- Equipping our developers with security tools, such as the Open Web Application Security Project (OWASP) and Agile methodology, to leverage early in the System Development Life Cycle (SDLC) process. Blackbaud applications are developed using industry-standard best practices throughout the SDLC. Our development teams use the Agile software development methodology for guiding their planning and process management and utilize the Open Web Application Security Project (OWASP) "Top 10" list for secure coding practices. All applications undergo stringent Quality Assurance (QA) testing before being delivered to our network engineers for deployment to our production environment. This testing includes both static code scanning and dynamic vulnerability scanning in our simulated testing network. Blackbaud's development, QA, and staging environments are strictly segregated from the production environment in our hosting facility.
- We incorporate a "security by design" posture throughout our development processes across our portfolio, starting with defensible network architecture. For web and mobile, we primarily use the OWASP SKF for our SDLC, and all developers are engaged in ongoing training on secure software development best practices.
- A security liaison is engaged early in the design process to facilitate our DevSecOps delivery model, which integrates security practices into a DevOps software delivery model, enables Blackbaud to serve customers at a faster pace, and ensures security is built into our applications by design.
- All access to infrastructure follows best practice Multi-Factor Authentication (MFA). Access is highly controlled and limited in scope and breadth. For solutions behind Blackbaud ID, we support MFA and modern identity providers (IdP) such as Microsoft Azure Active Directory, Okta, and SAML-based providers, allowing you to control your end-user login experience.

TESTING

Blackbaud's Global Trust and Security Team prioritizes routine testing to identify and remediate vulnerabilities and risks by leveraging:

- The F.A.I.R. Risk Management Framework
- The NIST Cybersecurity Framework
- A dedicated Red Team serves the entire organization by finding and exploiting security vulnerabilities and exploring the potential degree of impact with the goal of improving Blackbaud's security posture.
- Static Code Analysis
- Dynamic Application Testing
- Software Component Analysis
- Routine Penetration Testing
- Regular Code and Vulnerability Scanning and Assessments
- Distributed Denial-of-Service (DDoS) attack auto mitigation
- Cloud Audits and Assessments
- Phishing Simulations
- A robust Cybersecurity Incident Response Program is aligned with industry standard practices to identify, contain, eradicate, and recover from inevitable security incidents.

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 relevant global data privacy regulations and legislation to ensure our products and practices are aligned with relevant privacy legislation, as well as share best practices on the operational impact of these regulations and compliance requirements.

Continued on next page...

Further, we continue to work on ways to improve the user experience in our products, specifically regarding 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), regulations in the United Kingdom and the European Union that establish commercial standards for data protection and privacy for all individuals in those areas.
  - Learn more about Blackbaud's GDPR compliance and view GDPR Documentation according to your specific Blackbaud product.
- US State data privacy laws—including the California Consumer Privacy Act as amended by the California Privacy Rights Act—which enhance privacy rights and consumer protection for residents of those states.
  - We have made changes here at Blackbaud for our own compliance with these new state laws, particularly with respect to our Data Intelligence business. We have prepared new notices, implemented mechanisms for individuals to submit consumer rights requests, and readied our engineers to create robust subject access reports upon request. Blackbaud acts as a data controller when it provides Data Intelligence services, including Target Analytics®, and accordingly will comply with consumers' access requests, deletion requests, and opt out requests. Individuals who opt out of the sale of their data will be excluded from the data sets we use for customer data enrichment services. For more information, refer to our website for Data Subject Rights Requests as well as our Privacy Policy.
- Global email laws, such as Canada's Anti-Spam Legislation (CAN-SPAM) in the US, and the UK's Privacy and Electronic Communications Regulations (PECR) 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. For more information about safeguarding your constituent data, reference the Blackbaud Institute's Privacy Toolkit.

PARTNERSHIP

We are committed to championing your organization's security, starting with our own transparency and responsiveness, and acting as a strong partner across the social good and cybersecurity communities more broadly.

TRANSPARENCY

Blackbaud proactively publishes industry-standard third-party security audit reports 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. Many of these security reports and attestations available to you in our Compliance Portal. Compliance certifications and assessments may vary by product.

We produce white papers on our security approach and practices. We also help you strengthen your first line of defense against security threats by providing free best practices resources and Tip Sheets.

Blackbaud provides regular Product Update Briefings where you can interact with product managers and other experts on how we are continuing to keep your security at the center of our roadmaps.

EXPERT AFFILIATIONS

Blackbaud is an active consumer—and influencer—of cyberscurity thought leadership communities, including:

- Blackbaud is a member of Cloud Security Alliance (CSA) and assesses our products and environments against the CSA Consensus Assessment Initiative Questionnaire (CAIQ). Blackbaud leverages the Cloud Security Alliance's CAIQ to provide transparency regarding the adherence of our products to the CSA Cloud Controls Matrix. These assessments are made available via the CSA.

Continued on next page...

- Blackbaud's Global Trust and Security Team 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/NGOs under attack from sophisticated threat actors.
- Blackbaud security leaders partner with other experts across the field, benefiting from shared expertise, sharing information and strengthening the community as a whole, on the newly-created Institute for Security & Technology Ransomware Task Force.
- Blackbaud leverages tactical cybersecurity 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
- Partnerships with other cloud providers and independent third parties for reviews
- Robust and continuous Cloud Account/Subscription Governance and control monitoring
  - Blackbaud utilizes System Center Operations Manager (SCOM) and Azure Monitor for internal out-of-the-box monitoring with customized management packs that monitor within the application layer from the inside out.
  - An early warning detection system allows adequate time to investigate and respond to an issue before it becomes an impactful event.
  - Blackbaud augments the robust expertise of our own team with additional capacity through partnership with a leading Managed Security Service Provider (MSSP) for 24/7/365, offering continuous security monitoring, threat intelligence, and incident response support, as well as continued partnerships with security forensics professionals/companies and partnership with an industry-leading threat intelligence and dark web monitoring provider.

RELIABILITY

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

EXPERTISE

Every employee at Blackbaud receives ongoing security training, including required annual certification for each employee worldwide, to protect both Blackbaud's and our customers' data. All employees are provided continual phishing simulation testing to increase their awareness of cybersecurity social engineering and phishing techniques. Additional targeted training is provided to employees based on their job functions, including ongoing training on secure code development leveraging the OWASP top ten for all developers.

Blackbaud's Global Trust and Security Team partakes in worldwide communities and conference platforms—such as bbcon, Women in Cybersecurity (WiCyS), and local security conferences—to share information and present on industry best practices to improve the community's security awareness posture.

Conclusion

With Blackbaud's Cloud Operations, your team can work smarter and increase productivity, adoption, and reporting that speaks your language! Expand your impact with essential software created specifically for organizations like yours. In an ever-evolving threat landscape, you need a partner who will help you keep your focus on what matters most—your mission.