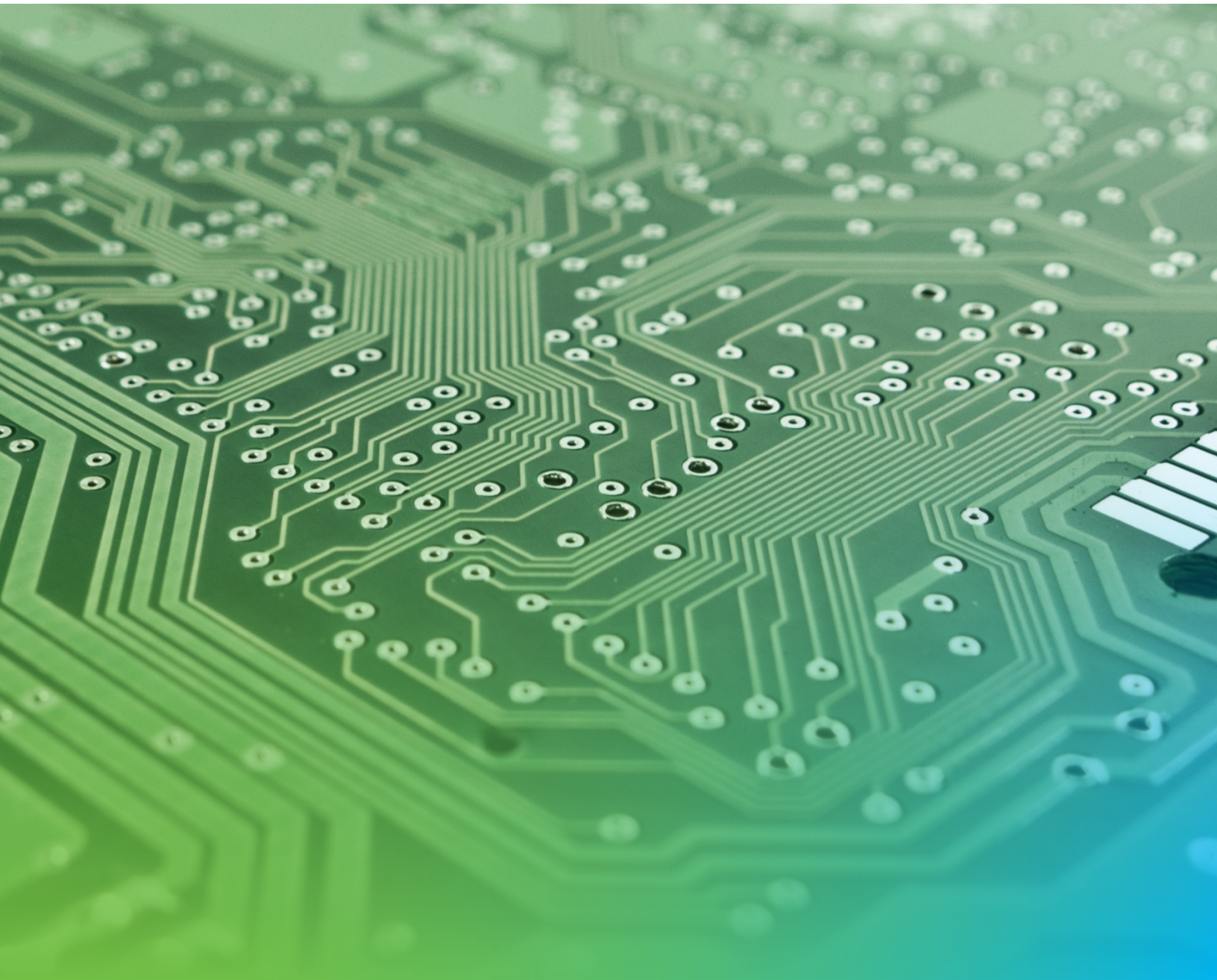
blackbaud

Blackbaud Cyber Security Program and Policy Framework

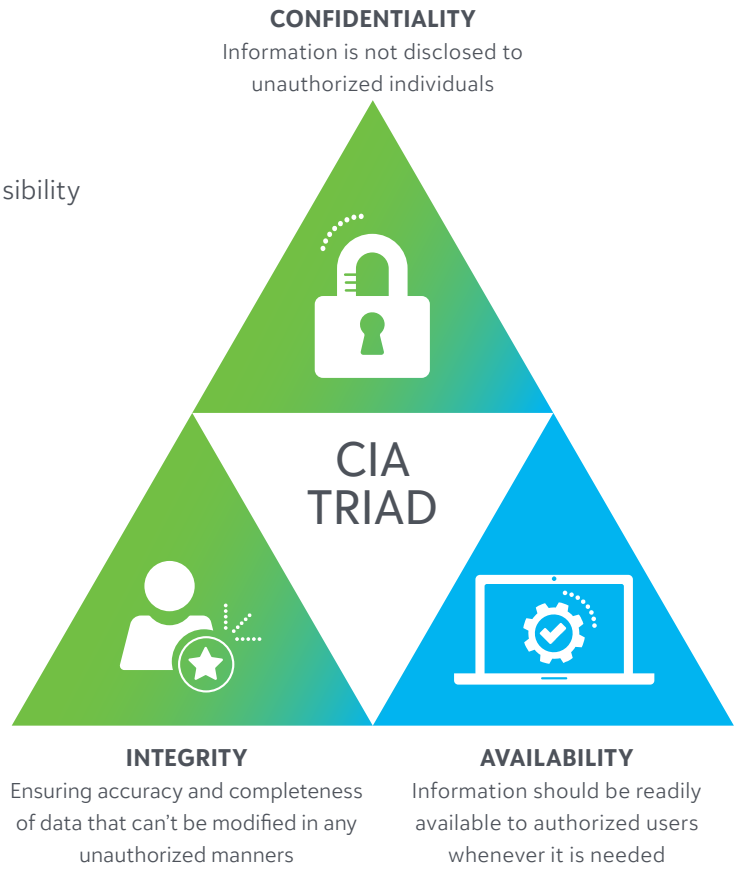


Blackbaud strives to provide industry-leading software solutions designed to support the unique needs of nonprofit and social good organizations with a heightened focus on Cyber Security. Blackbaud's robust Cyber Security team models the Cyber Security program to align with many industry control frameworks, compliance regulations, privacy requirements, and best practices.

Policy Parameters

Modeled after PCI DSS and ISO 27001 Governance structures, and considering the CIA Triad Model of information security (Confidentiality, Integrity, Availability), Blackbaud has implemented policies, procedures, and standards to address the following areas :

- Overarching Cyber Security Practices
- Cyber Security Non-Functional Requirements
- Security Awareness Training and Employee responsibility
- Secure Acceptable Use
- Information Classification
- Data Protection & Retention
- Access Control Standards
- Physical and Environmental Security
- Network & Telecommunications Security
- Incident Management
- Secure SDLC Policy & Standards
- Vulnerability Management
- Change and Configuration Management
- Risk Management
- Business Continuity & Disaster Recovery



© November 2022, Blackbaud, Inc.

This white paper is for informational purposes only. Blackbaud makes no 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.

Continued on next page...

Policy Purposes

We have designed these policies and standards to accomplish the following (in alignment with CIA Triad):

CONFIDENTIALITY

Confidentiality of your data is enforced by access levels for all information and information processing systems. Blackbaud's policies, procedures, and controls establish safeguards for your data, whether sensitive or confidential, from unauthorized access.

INTEGRITY

We ensure the accuracy and completeness of data that cannot be modified in any unauthorized manner. Blackbaud's policies and procedures ensure your data is protected from deletion or modification from any unauthorized party, and also ensures any inadvertent changes you make can be reversed.

AVAILABILITY

Your information should be readily available to authorized users whenever it is needed. Blackbaud has established policies, processes, and controls encompassing a continued effort of assurance that you have access to your data whenever necessary.

ACCOUNTABILITY

Accountability at Blackbaud embodies all operations. This includes people, information systems, and processes which are identified in Blackbaud's policies and procedures. Our collective security monitoring capabilities assure data is identified and traceable to an original author.

ASSURANCE

Blackbaud's policies and procedures require technical and operational security measures to assure the protection and risk management of information systems and your data.

Policy Protocol

Blackbaud assesses its Cyber Security program continuously, with annual updates and training to our employees of any changes to the above policies and standards. We also work continuously with our employees to ensure the above policies are understood and adhered to, which enhances our ability to design and continue to improve secure solutions for our customers.

Program Framework Assessments

Blackbaud assesses its environments and products regularly against many industry standard frameworks and best practices, including:

- NIST CSF
- PCI DSS
- SOC 1
- SOC 2
- GDPR
- HIPAA
- Trans-Atlantic Data Privacy Framework
- Cloud Security Alliance

Continued on next page...

On a routine basis, the Blackbaud Cyber Security team assesses the maturity of its cyber security program specifically utilizing the National Institute of Standards and Technology (NIST) Cyber Security Framework.

This framework details controls related to the following areas of Cyber Security Maturity:

Function	Goal	Categories Affected
IDENTIFY	Develop Blackbaud's ability to understand and manage cyber security risks to information assets and data.	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management
PROTECT	Allow Blackbaud to implement and further improve safeguards which ensure information is protected appropriately throughout the delivery of our solutions.	• Identity Management • Authentication and Access Control • Awareness & Training • Data Security • Information Protection & Procedures • Maintenance • Protective Technology
DETECT	Mature Blackbaud's ability to identify cyber security events swiftly and mitigate risk	• Anomalies & Events • Security Continuous Monitoring • Detection Process
RESPOND	Mature Blackbaud's ability to take immediate action in response to any cyber security events detected	• Response Planning • Communications • Analysis • Mitigation • Improvements
RECOVER	Enable Blackbaud to take appropriate and timely actions to minimizes impact to our customers and recover from any potential cyber security events	• Anomalies & Events • Security Continuous Monitoring • Detection Process

For more information, visit www.nist.gov/cyberframework

Learn more

Continued on next page...

Conclusion

Blackbaud leverages detailed frameworks, programs, and compliance standards to ensure that the solutions we deliver to our customers are best in breed and meeting strong cyber security requirements and standards outlined by various governmental and regulatory industry entities.

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 Consensus Assessments Initiative Questionnaire (CAIQ) 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.

For more information on Blackbaud's security measures, visit blackbaud.com/security.

Learn more

About Blackbaud
Leading uniquely at the intersection point of technology and social good, Blackbaud connects and empowers organizations to increase their impact through cloud software, services, expertise, and data intelligence. We serve the entire social good community, which includes nonprofits, foundations, companies, education institutions, healthcare organizations, and the individual change agents who support them.