ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance ("Assurance")[1] is entered into by the Consumer Protection Division of the Office of the Attorney General of Maryland (the "Division")[2] and Blackbaud, Inc., including all of its United States subsidiaries, affiliates, agents, representatives, employees, successors, and assigns ("Blackbaud", and together with the State, the "Parties") to resolve the investigation of the Attorneys General of the **Breach** first publicly announced by Blackbaud on July 16, 2020. The investigation examined the facts and circumstances surrounding the **Breach** and whether Blackbaud complied with the State of Maryland's unfair or deceptive acts and practices law ("**Consumer Protection Law**"), and personal information protection law ("**Personal Information Protection Law**"), as well as the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226 ("**HIPAA**") (collectively, the "**Relevant Laws**"). In consideration of their mutual agreements to

[1] This Assurance of Voluntary Compliance shall, for all necessary purposes, also be considered an Assurance of Discontinuance.

[2] Blackbaud is simultaneously entering into similar agreements with the Attorneys General of Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. For ease of reference, this entire group will be referred to collectively herein as the "Attorneys General" or individually as "Attorney General." Such designations, however, as they pertain to Connecticut, shall refer to the Attorney General, both acting on his own behalf and as authorized by the Commissioner of the Department of Consumer Protection. Such designations, as they pertain to Hawaii, shall refer to both the Attorney General and the Executive Director of the State of Hawaii Office of Consumer Protection. Such designations, as they pertain to Maryland, shall refer to the Consumer Protection Division of the Office of the Attorney General of Maryland, which has authority to enter into this Assurance pursuant to Md. Code Ann., Com. Law § 13-402. Each State's Assurance incorporates the substantive terms included herein. To the extent there are differences, those differences arise from the requirements of local rules and state laws.

the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby enter this Assurance and agree as follows:

I. PARTIES AND JURISDICTION

1. The Division is charged with enforcement of the **Relevant Laws** of this State, and pursuant to 42 U.S.C. § 1320d-5(d), may also enforce **HIPAA**.

2. Blackbaud, a Delaware corporation headquartered in Charleston, South Carolina, provides donor relationship management software to various organizations, including charities, higher education institutions, K-12 schools, healthcare organizations, religious organizations, and cultural organizations.

3. At all relevant times, Blackbaud was engaged in trade and commerce affecting consumers in the State of Maryland insofar as Blackbaud provides software and related services to **Blackbaud Customers**, including fraternal, religious, civil, patriotic, educational, or charitable organizations, which **Blackbaud Customers** use to connect with donors in the State. Blackbaud also stored the **Personal Information** and/or **Protected Health Information** of Maryland residents to the extent **Blackbaud Customers** decide to store such **Personal Information** and/or **Protected Health Information** in connection with **Blackbaud Customers'** use of Blackbaud's products and services.

4. Insofar as Blackbaud provided or provides products or services to **Blackbaud Customers** that are **Covered Entities** and to the extent **Blackbaud Customers** that are **Covered Entities** decide to store **Protected Health Information** in connection with such **Blackbaud Customers'** use of Blackbaud's products and services, Blackbaud is a **Business Associate** subject to the requirements of **HIPAA**.

II. ATTORNEY GENERAL FINDINGS

5. Blackbaud provides software that organizations use to connect with donors and manage data about their donors, including identifying information, donation history, and financial information. On May 14, 2020, Blackbaud discovered a ransomware attack that resulted in the unauthorized access and exfiltration of sensitive donor information. On July 16, 2020, Blackbaud publicly announced the incident and began notifying impacted customers. Thereafter, Blackbaud's customers notified impacted donors across the United States, including Maryland residents, of the **2020 Data Breach**. The **2020 Data Breach** affected over a million files related to over 13,000, or roughly a quarter, of Blackbaud's customers.

III. DEFINITIONS

For the purposes of this Assurance, the following definitions shall apply:

6. "**2020 Data Breach**" shall mean the **Security Incident**, first publicly announced by Blackbaud on July 16, 2020, in which a person or persons gained unauthorized access to the **Blackbaud Network**.

7. "**Blackbaud User**" shall mean any employee, representative, contractor, subcontractor or agent of Blackbaud for whom Blackbaud has created a user account and credentials to access the **Blackbaud Network**.

8. "**Blackbaud Customer**" shall mean any entity[3] that has contracted with Blackbaud to receive Blackbaud products and/or services and has stored **Personal Information** and/or **Protected Health Information** in connection with the use of such products and/or services.

9. "**Blackbaud Network**" shall mean all networking equipment, technical

[3] The entities that Blackbaud provided services to are defined as "Consumers" under Md. Code, Com. Law § 13-101(c)(iv). For purposes of this Assurance, such "Consumers" are considered **Blackbaud Customers** herein.

infrastructure relating to on-prem, cloud-based, and/or colo databases or data stores, applications, servers, and endpoints that: (a) are capable of using and sharing software, data, and hardware resources; (b) are owned, operated, and/or controlled by Blackbaud; and (c) process, store, or have access to **Personal Information** and/or **Protected Health Information** of **Consumers** who reside in the United States.

10. "**Business Associate**" shall be defined in accordance with 45 C.F.R. § 160.103.

11. "**Clearly and Conspicuously**" shall mean that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by **Blackbaud Customers**, including in all of the following ways:

a. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a video, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made through only one means.

b. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

c. An audible disclosure, including by telephone or video, must be delivered in a volume, speed, and cadence sufficient for representatives of **Blackbaud Customers** to easily hear and understand it.

d. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable (hard to miss).

e. The disclosure must use understandable language, diction, and syntax.

f. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

g. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

12. "**Compensating Controls**" shall mean alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the **Chief Information Security Officer** or his or her designee to be impractical or unreasonable to implement at the applicable time due to legitimate technical or business constraints. Such alternative mechanisms must: (a) meet the intent and rigor of the original stated requirement; (b) provide a similar level of security as the original stated requirement; (c) be materially and substantively up-to-date with current industry accepted security protocols; and (d) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the **Chief Information Security Officer** or his or her designee agrees with both the risk analysis and the determination that the risk is acceptable. **Compensating Controls** shall not be utilized as permanent alternative security measures and shall be reevaluated for security effectiveness at least every ninety (90) days to determine whether to retain the **Compensating Control** as the appropriate security measure or to implement an alternative as the permanent security measure. Written security effectiveness documentation shall be prepared and reviewed by the **Chief Information Security Officer** or his

or her designee and shall be kept for a period of one (1) year following the termination of usage of any such alternative mechanism.

13. "**Consumer**" shall mean any individual whose **Personal Information** and/or **Protected Health Information** is processed, stored, or otherwise made accessible on behalf of **Blackbaud Customers** on the **Blackbaud Network**. This definition excludes (i) Blackbaud employees, directors, representatives, contractors, subcontractors, agents and their dependents as well as (ii) the business contact information of **Blackbaud Customer** employees or authorized agents that is stored on Blackbaud corporate systems.

14. "**Consumer Protection Law**" shall mean the Maryland citation(s) set forth in Exhibit A.

15. "**Covered Entity**" shall be defined in accordance with 45 C.F.R. § 160.103.

16. "**Effective Date**" shall be November 6, 2023, except as otherwise noted in the Assurance.

17. "**Encrypt**", "**Encrypted**" or "**Encryption**" shall mean encoding data into ciphertext—at rest or in transit—rendering it unusable, unreadable, or indecipherable without converting the ciphertext to plaintext, through the use of a reasonable confidential process and key, leveraging a security technology, methodology, or encryption algorithm commensurate with the sensitivity of the data at issue.

18. "**Governance Process**" shall mean any written policy, standard, procedure, or process (or any combination thereof) designed to achieve a control objective with respect to the **Blackbaud Network**.

19. "**Personal Information**" or "**PI**" shall mean information regarding a **Consumer** residing in Maryland that falls within one of the following categories:

a. A first name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (i) Social Security number; (ii) driver's license number; (iii) state- or federally-issued identification card number; or (iv) financial account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the consumer's financial account;

b. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical characteristics or digital representation thereof;

c. A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account; or

d. Any category of personal information found in the definition set forth in the **Personal Information Protection Law**.

20. "**Personal Information Protection Law**" shall mean the Maryland citation(s) set forth in Exhibit A.

21. "**Protected Health Information**" or "**PHI**" shall mean the Protected Health Information or PHI, as defined in accordance with 45 C.F.R. § 160.103, of a **Consumer**.

22. "**Security Incident**" shall mean any compromise, or imminent threat of a compromise to the confidentiality, integrity, or availability of **PI** or **PHI** stored within, accessed, or transmitted through the **Blackbaud Network**, by unauthorized access or inadvertent disclosure, including but not limited to an incident for which notification may be required under the **Personal Information Protection Law** or **HIPAA**. For purposes of this definition, "availability" shall not

include an intentional limitation on the availability of **PI** or **PHI**, such as for purposes of performing maintenance on the **Blackbaud Network**.

IV. INJUNCTIVE RELIEF

23. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to Blackbaud and its directors, officers, and employees.

24. The injunctive terms contained in this Assurance are entered pursuant to Md. Com. Law § 13-402.

A. COMPLIANCE WITH LAW

25. Blackbaud shall comply with the **Consumer Protection Law** and **Personal Information Protection Law** in connection with its processing, storing and safeguarding of **PI** and/or **PHI**.

26. Blackbaud shall comply with the **Personal Information Protection Law in connection with breach notification**, as applicable.

27. Blackbaud shall comply with **HIPAA**, as applicable, including the Privacy Rule (45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E) and Security Rule (45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C), and shall implement all Administrative, Technical, and Physical Safeguards required by **HIPAA**. "Administrative Safeguards", "Technical Safeguards" and "Physical Safeguards" shall be defined in accordance with 45 C.F.R. §§ 164.304, 164.308, 164.310, 164.312.

28. Blackbaud shall not make a misrepresentation which is capable of misleading **Blackbaud Customers** or **Consumers**, or fail to state a material fact if that failure is capable of misleading **Blackbaud Customers** or **Consumers**, regarding the extent to which Blackbaud

maintains and/or protects the privacy, security, confidentiality, or integrity of **PI** or **PHI** of **Consumers**.

29. Blackbaud shall not make a misrepresentation which is capable of misleading **Blackbaud Customers** or **Consumers**, or fail to state a material fact if that failure is capable of misleading **Blackbaud Customers** or **Consumers**, regarding the likelihood that **PI** or **PHI** affected by a **Security Incident** may be subject to further unauthorized access, disclosure or other misuse.

30. Blackbaud shall not misrepresent to **Blackbaud Customers** the notification requirements of the **Data Breach Notification Law** or **HIPAA**.

B. INCIDENT RESPONSE PLAN

31. Blackbaud shall implement and maintain written incident response plan(s) to prepare for and respond to **Security Incidents** ("**Incident Response Plan**"). Blackbaud shall investigate **Security Incidents**. Blackbaud shall maintain documentation sufficient to show the investigative and responsive actions taken in connection with each **Security Incident** and the determination as to whether notification under the **Data Breach Notification Law** or **HIPAA** is required. Blackbaud shall also assess whether there are reasonably feasible training or technical measures, in addition to those already in place, that would materially decrease the risk of the same type of Security Incident from reoccurring. Blackbaud shall revise and update the **Incident Response Plan**, as necessary, to adapt to any changes to the **Blackbaud Network**. Such a plan shall, at a minimum, identify and describe the following phases:

a. Preparation;

b. Detection and Analysis;

c. Containment;

d. Eradication;

e. Recovery; and

f. Post-Incident Analysis and Remediation.

32. Blackbaud shall conduct, at a minimum, exercises ("table-top exercises") twice a year to test and assess its preparedness to respond to a **Security Incident**.

C. BREACH RESPONSE AND NOTIFICATION

33. Blackbaud shall implement and maintain a **Breach** response plan (as defined below) that contains policies and procedures for (a) notification and coordination with law enforcement, as appropriate, and **Blackbaud Customers**; (b) affected **Blackbaud Customer** response (including consideration of appropriate staffing levels, training, and written materials); and (c) regulator notification, as applicable.

34. Blackbaud shall conduct, at a minimum, exercises ("table-top exercises") twice a year to test and assess its preparedness to respond to a **Breach**. These exercises shall include the following, as appropriate:

a. Planning for sufficient staffing levels to handle a high volume of questions from affected **Blackbaud Customers** and to provide **Blackbaud Customers** with information in a reasonable amount of time;

b. Planning employee training to provide relevant, useful, and accurate information to **Blackbaud Customers**;

c. Preparing written materials to provide to **Blackbaud Customers** that **Clearly and Conspicuously** disclose relevant information.

35. In determining whether notification to **Blackbaud Customers** under the Personal Information Protection Law or **HIPAA** is required, Blackbaud shall consider information stored

by affected **Blackbaud Customers**, including information stored in fields not intended for **PI** and/or **PHI** in the affected Blackbaud products. Blackbaud shall also offer **Blackbaud Customers** reasonable guidance, cooperation and/or assistance, including with respect to instructions on how to run queries and reports of **Blackbaud Customer** databases affected by the **Security Incident** so that **Blackbaud Customers** can determine whether they must provide notification to **Consumers** in time to allow such notification in accordance with the Personal Information Protection Law or **HIPAA**. If after a **Blackbaud Customer** has sought and received such guidance, cooperation and/or assistance, the **Blackbaud Customer** is unable to run such queries and reports itself, Blackbaud shall reasonably run such queries and reports for the **Blackbaud Customers** at no cost, if requested by the **Blackbaud Customer**.

36. If Blackbaud determines that a **Security Incident** does not require notification under the **Personal Information Protection Law** or **HIPAA**, Blackbaud shall create documentation that includes a description of the **Security Incident** and Blackbaud's response to that **Security Incident** ("**Security Incident Report**"). Blackbaud shall make any **Security Incident Report** available to the Attorneys General upon written request.

37. In the case that a **Security Incident** requires notification under the **Personal Information Protection Law** or **HIPAA** ("**Breach**"), Blackbaud shall do the following:

a. Blackbaud shall timely notify affected **Blackbaud Customers** in accordance with the **Personal Information Protection Law**, **HIPAA**, and any applicable contracts with **Blackbaud Customers**.

b. Consistent with Blackbaud's obligations set forth in Paragraphs 35 and 37(c), Blackbaud shall **Clearly and Conspicuously** provide affected **Blackbaud Customers** with such information that each **Blackbaud Customer** requires to

provide timely notice to affected **Consumers** and the Attorneys General in accordance with the **Personal Information Protection Law** and **HIPAA**, as applicable.

c. To the extent possible and consistent with the mutually agreed roles and responsibilities under the applicable contract between Blackbaud and a **Blackbaud Customer**, if the identity of affected **Consumers** cannot be determined by a **Blackbaud Customer** following Blackbaud's provision of the guidance and/or assistance set forth in Paragraph 35 of this Assurance, Blackbaud shall assist **Blackbaud Customers** in determining the names of affected **Consumers** in such **Blackbaud Customer's** affected databases.

d. Blackbaud shall specify in any new contracts entered into with **Blackbaud Customers** after the **Effective Date** the roles and responsibilities to be undertaken by Blackbaud and the **Blackbaud Customer** in the event of a **Breach**, specifically for providing notice to affected **Consumers** and the Attorneys General, as required by the **Personal Information Protection Law** or **HIPAA**, as appropriate.

D. INFORMATION SECURITY PROGRAM

38. Blackbaud may satisfy the requirements to implement and maintain a comprehensive information security program ("**Information Security Program**"), including the written incident response plan and other specific information security requirements noted below and elsewhere herein, through review, maintenance, and as necessary, updating of Blackbaud's existing information security program and related safeguards, provided that such program and safeguards meet the requirements of this Assurance. Unless otherwise specified herein, within ninety (90) days after the **Effective Date**, Blackbaud shall implement, maintain, periodically

review and revise, and comply with an **Information Security Program** the purpose of which shall be to take reasonable steps to protect the confidentiality, integrity, and availability of **PI** and **PHI** on the **Blackbaud Network**. Blackbaud's **Information Security Program** shall be documented in the **Governance Processes** and shall contain administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of Blackbaud's operations;

b. The nature and scope of Blackbaud's activities; and

c. The sensitivity of the **PI** and **PHI** on the **Blackbaud Network**.

The **Information Security Program** required by this Assurance shall include the requirements of Paragraphs 39 through 70 in this Assurance. Should Blackbaud acquire any other entity and/or product, Blackbaud shall perform cybersecurity due diligence to assess such entity's/product's compliance with this Assurance. Blackbaud shall evaluate the requirements that must be met before the entity and/or product is integrated into the **Blackbaud Network,** including an assessment of whether the entity and/or product meets the requirements of this Assurance and all deficiencies requiring remediation, and Blackbaud shall develop an integration plan reflecting this analysis. After Blackbaud has assured itself of such entity's/product's compliance, and not later than two (2) years after the closing of such acquisition, the acquired entity/product shall be incorporated into the **Information Security Program** herein. Blackbaud shall document the cybersecurity due diligence required by this Paragraph for each acquisition, which shall be provided to the Attorneys General upon request.

39. Blackbaud shall implement appropriate access controls, including without limitation, least privileged access to only allow authorized users access to necessary resources on the **Blackbaud Network** for the organization's business needs, consistent with NIST Special

Publication 800-53 (page 36-39, AC-6), and zero-trust architecture, consistent with NIST Special Publication 800-207, where technically feasible and commercially reasonable.

40. Blackbaud shall reasonably oversee its third-party vendors who have access to the **Blackbaud Network** or who hold or store **PI** or **PHI** on Blackbaud's behalf by maintaining and periodically reviewing and revising, as needed, a **Governance Process** for assessing vendor compliance in accordance with Blackbaud's **Information Security Program** including whether the vendor's security safeguards are appropriate for that business. That **Governance Process** shall require vendors in contracts entered into or renewed beginning ninety (90) days after the **Effective Date** to implement and maintain appropriate safeguards, and further require Blackbaud to make commercially reasonable efforts to require vendors to notify Blackbaud within seventy-two (72) hours of discovering any security incident that may give rise to a **Breach** (a "**Third-Party Reported Incident**"). At a minimum, the Governance Process shall require vendors in contracts entered into or renewed beginning ninety (90) days after the **Effective Date** to notify Blackbaud within five (5) business days of discovering any **Third-Party Reported Incident**.

41. Blackbaud shall employ an individual who shall be responsible for implementation of Blackbaud **Governance Processes** relating to compliance with privacy laws, including the **Personal Information Protection Law** and **HIPAA** (hereinafter referred to as the "**Chief Privacy Officer**"). The **Chief Privacy Officer** shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role, and possess a fundamental understanding of state and federal privacy and data security laws;

b. Assist Blackbaud in complying with **Personal Information Protection Law** and **HIPAA**; matters related to Blackbaud's privacy compliance assessments; and

coordination with Blackbaud executives and officers as it relates to business operations affecting the privacy, confidentiality, integrity, and security of **PI** and **PHI** in the **Blackbaud Network**; and

c. Provide reports as necessary to the Office of General Counsel, which shall provide reports as necessary to the Chief Executive Officer, and as necessary, to the Board of Directors.

42. Blackbaud shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the **Information Security Program** (hereinafter referred to as the "**Chief Information Security Officer**"). The **Chief Information Security Officer** shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role in implementing, maintaining, and monitoring the **Information Security Program**;

b. Provide an annual report to the Blackbaud Board of Directors on the adequacy of Blackbaud's **Information Security Program**;

c. At any meeting of the Board of Directors concerning the security posture or security risks faced by Blackbaud, provide reports to Blackbaud's Board of Directors, and shall inform, advise, and update the Board of Directors regarding Blackbaud's security posture and the security risks faced by Blackbaud; and

d. Notify the Chief Executive Officer of any **Security Incident** or **Third-Party Reported Incident** involving over ten (10) **Blackbaud Customers** within forty-eight (48) hours of discovery, as well as notify a member of Blackbaud's Board of

Directors, in the event that the Chief Executive Officer is not a member of the Board of Directors, within seventy-two (72) hours of discovery.

43. Blackbaud shall employ one or more individuals to serve as liaison between areas of Blackbaud business and the office of the **Chief Information Security Officer** regarding implementation, maintenance, and monitoring of the **Information Security Program** for the area of Blackbaud business (hereinafter referred to as a "**Business Information Security Officer**"). Each **Business Information Security Officer** shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of the **Business Information Security Officer**'s role in implementing, maintaining and monitoring the **Information Security Program**; and

b. Be responsible for regularly informing, advising, and updating the **Chief Information Security Officer** or his or her designee regarding the security posture of the areas of Blackbaud business for which he or she is responsible for liaising; the security risks faced by the relevant area of Blackbaud business; and the implications of any decision the **Business Information Security Officer** makes that may materially impact the security posture of the area of Blackbaud business.

44. Blackbaud shall employ one or more individuals who shall be responsible for developing, maintaining, and monitoring the information technology needs and requirements of Blackbaud's staff, operations, network, and devices (hereinafter may be referred to as the "**Chief Technology Officer**"). Such individuals shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role in developing, maintaining, and monitoring the

information technology needs and requirements of Blackbaud's staff, operations, network, and devices;

b. Develop and execute the company's strategy for utilizing technological resources, with the goal of ensuring that all Blackbaud technological resources are up-to-date and patched accordingly, and supervise the **Patch Supervisor**; and

c. Provide reports as necessary to the Chief Executive Officer and coordinate with the **Chief Privacy Officer and Cybersecurity Counsel** and **Chief Information Security Officer**, to take steps to ensure Blackbaud's information technology, information security, and privacy programs are cohesive and aligned.

45. Blackbaud shall provide the **Chief Privacy Officer**, **Chief Information Security Officer**, **Business Information Security Officers, Chief Technology Officer, Information Security Program** and corresponding cybersecurity staff with the resources and support reasonably necessary so that the **Information Security Program** functions as required by this Assurance.

46. Without limiting the foregoing, Blackbaud may fulfill the specified governance roles and responsibilities in this Assurance with individuals with titles that do not directly correspond to the defined terms in this Assurance; provided that Blackbaud meets the functional requirements of Paragraphs 41-45.

E. TRAINING REQUIREMENTS

47. Employees who are responsible for implementing, maintaining, or monitoring the **Information Security Program**, including but not limited to the **Chief Information Security Officer** and **Business Information Security Officers**, shall receive specialized training to help effectuate Blackbaud's compliance with the terms of this Assurance. Blackbaud shall provide the

training required under this Paragraph to all such employees within ninety (90) days of the **Effective Date** of this Assurance or prior to an employee starting their responsibilities for implementing, maintaining, or monitoring the **Information Security Program**. Blackbaud shall document the trainings, including the date(s) upon which they were provided and to whom.

48. Blackbaud shall provide training on safeguarding and protecting **PI** and **PHI** to its employees who handle **PI** or **PHI**, and its employees responsible for implementing, maintaining, or monitoring the **Information Security Program**. Such training shall be appropriate to employees' job responsibilities and functions and shall occur on an annual basis, or more frequently if appropriate, beginning within ninety (90) days of the **Effective Date** of this Assurance or prior to an employee handling **PI** or **PHI** or starting their responsibilities for implementing, maintaining, or monitoring the **Information Security Program**. Blackbaud shall document the trainings, including the date(s) upon which they were provided and to whom.

49. Blackbaud shall provide specialized technology and cybersecurity training, ongoing education, and product training to relevant information technology and information security personnel.

F. PERSONAL AND PROTECTED HEALTH INFORMATION SAFEGUARDS AND CONTROLS

50. Blackbaud shall maintain and comply with a **Governance Process** establishing that **Blackbaud Customer** database backup files containing **PI** and **PHI** will be stored to the minimum extent necessary to accomplish Blackbaud's intended legitimate business purpose(s) in storing the information in such database backup files on behalf of **Blackbaud Customers**. With respect to **PHI**, the **Governance Process** shall be consistent with the Minimum Necessary Standard, which shall refer to the requirements of the Privacy Rule that, when using, disclosing, or requesting **PHI**, a **Covered Entity** or **Business Associate** must make reasonable efforts to limit **PHI** to the

minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).

51. Blackbaud shall maintain, regularly review and revise as necessary, and comply with the **Governance Process** to appropriately protect **PI** and **PHI** from unauthorized access whether the information is transmitted electronically from the **Blackbaud Network** or stored in the **Blackbaud Network**. Any such **Governance Process** shall include at a minimum, total database encryption of all databases that contain **Blackbaud Customer** data. Where appropriate, and until total database encryption of all databases is completed, field-level encryption of data fields that may include **PI** and/or **PHI** shall continue. Blackbaud shall also require all third-party data storage or cloud providers to apply equal to or greater encryption protocols to any **Blackbaud Network** data.

52. Blackbaud shall maintain, regularly review and revise as necessary, and comply with the **Governance Process** that provides for the secure disposal, on a periodic basis, of **Blackbaud Customer** database backup files within Blackbaud's control in accordance with written retention schedules.

53. Blackbaud shall invest in and utilize a solution for searching, monitoring, and tracking the dark web for **Blackbaud Network** data, including **Blackbaud Customer** data if there is a **Breach**. If **Blackbaud Network** data or a threat to **Blackbaud Network** data is discovered on the dark web, Blackbaud shall notify the **Chief Privacy Officer** and **Chief Information Security Officer**, who shall then notify the Office of General Counsel and Chief Executive Officer, and if applicable, any **Blackbaud Customers** whose data may be affected.

G. SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

54. Network Segmentation:

a. Blackbaud shall maintain, regularly review and revise as necessary, and comply with network segmentation protocols and related policies that are reasonably designed to properly segment the **Blackbaud Network** or otherwise implement **Compensating Controls**, which shall, at a minimum, comply with NIST CSF controls related to network segmentation.

b. Blackbaud shall regularly evaluate, and, as appropriate, restrict and/or disable any unnecessary ports on the **Blackbaud Network**.

c. Blackbaud shall logically separate its development, production and non-production environments in the **Blackbaud Network**.

d. Blackbaud shall employ microsegmentation and/or access control security principles in the **Blackbaud Network** at the following levels: (1) application; (2) database; (3) and user. The requirements of this Paragraph shall commence upon one hundred and eighty (180) days after the Effective Date.

55. Risk Assessment: Blackbaud shall maintain and regularly review and revise as necessary a risk-assessment program designed to identify and assess risks to the **Blackbaud Network**. Risk assessments shall follow the NIST Cybersecurity Framework, or where required and deemed appropriate, another established industry standard cybersecurity framework and be performed annually under the direction of the **Chief Information Security Officer** and Blackbaud's General Counsel and shall be documented. In cases where Blackbaud deems a risk to be acceptable, Blackbaud shall generate and retain for at least seven (7) years a record stating why Blackbaud deems the risk to be acceptable and demonstrating how such risk is to be managed

in consideration of cost or difficulty in implementing effective countermeasures. All reports shall be maintained by the **Chief Information Security Officer** or his or her designee and be available for inspection by the **Third-Party Assessor** described in Paragraph 69 of this Assurance when the **Third-Party Assessor** is conducting its **Third-Party Assessments**.

56. Penetration and Security Testing:

a. Within one hundred and eighty (180) days of the Effective Date, Blackbaud shall implement and maintain a risk-based security-testing program reasonably designed to identify, assess, and remediate security vulnerabilities within the **Blackbaud Network**. This program shall include: (i) testing for security vulnerabilities for Blackbaud developed applications before deployment to any public-facing webserver using static and dynamic application testing for production releases; (ii) at least one annual penetration test of all Blackbaud products; (iii) vulnerability scans of all systems in the **Blackbaud Network** occurring at least weekly; and (iv) vulnerability scans of the production environment of the **Blackbaud Network** within twenty-four (24) hours after any material modifications. All results shall be documented and maintained for two (2) years.

b. Blackbaud shall rate and rank the criticality of all vulnerabilities identified as a result of any vulnerability scanning or penetration testing that it performs on the **Blackbaud Network** in alignment with an established industry-standard framework (e.g., NVD, CVSS, or equivalent standard). For each vulnerability that is ranked as most critical, Blackbaud shall commence remediation planning within seventy-two (72) hours after the identification of the vulnerability and shall apply the remediation within fifteen (15) days after the identification of the vulnerability.

If the remediation cannot be applied within fifteen (15) days after the identification of the vulnerability, Blackbaud shall identify existing or implement new **Compensating Controls** designed to protect **PI** and **PHI** as soon as practicable but no later than fifteen (15) days after the identification of the vulnerability. All results shall be documented and maintained for three (3) years.

57. Access Control and Account Management:

a. Blackbaud shall implement and maintain appropriate controls to manage access to, and use of, all **Blackbaud User** accounts with access to **Blackbaud Customer** databases that store **Consumer** data, including, without limitation, individual accounts, administrator accounts, service accounts, and vendor accounts.

b. To the extent that Blackbaud maintains accounts requiring passwords:

i. Such controls shall be consistent with the requirements of NIST or another established industry standard cybersecurity framework, including reasonable password confidentiality and password-rotation policies; or multi-factor authentication, tokens, or any other equal or greater authentication protocol. For purposes of this Paragraph, any administrative-level passwords shall be **Encrypted** or secured using a reasonable password vault, privilege access monitoring, or other **Compensating Control**; and

ii. Blackbaud shall implement and maintain appropriate policies for the secure storage of **Blackbaud Network** account passwords based on industry accepted security practices; for example, hashing and salting passwords stored online using an appropriate hashing algorithm that is not

vulnerable to a collision attack together with an appropriate salting policy, or other equivalent or stronger protections.

c. Blackbaud shall implement and maintain appropriate access controls, processes, and procedures, the purpose of which shall be to grant access to the **Blackbaud Network** only after the **Blackbaud User**, or **Blackbaud Customer** user, as applicable, has been properly identified and authenticated.

d. For **Blackbaud Users** that are employees or independent contractors of Blackbaud, Blackbaud shall as soon as practicable and (i) within one (1) business day of the termination of the **Blackbaud User**'s employment or contract with Blackbaud for **Privileged Accounts**, or (ii) within three (3) business days of the termination of the **Blackbaud User**'s employment or contract with Blackbaud for standard accounts, terminate access for all such terminated **Blackbaud Users**. **Blackbaud User** accounts issued to a third party will be set to automatically expire whenever technically feasible for a period not to exceed one hundred and eighty (180) days from when the account was created. For purposes of this subsection, the date of termination shall be the date recorded by Blackbaud's Human Resources Department. "**Privileged Accounts**" shall mean accounts that provide the ability to make system and software configuration changes, perform administrative tasks, and create or modify **Blackbaud User** accounts. All access terminations shall be documented and maintained for five (5) years.

e. Blackbaud shall limit the access of **Blackbaud Users** to **Blackbaud Customer** databases that store **Consumer** data on a least-privileged basis.

f. Blackbaud shall regularly inventory the **Blackbaud Users** who have access to the **Blackbaud Network** in order to review and determine whether or not such access remains necessary or appropriate. Blackbaud shall compare termination lists to **Blackbaud User** accounts to determine whether access privileges have been appropriately terminated. At a minimum, such review shall compare termination lists to **Blackbaud User** accounts to determine whether access privileges have been appropriately terminated on a quarterly basis. The requirements of this subsection shall commence upon one hundred and eighty (180) days after the Effective Date.

g. Within one hundred and eighty (180) days of the Effective Date, Blackbaud shall implement Privileged Access Management (PAM) administration processes and procedures to store and monitor the account credentials and access privileges of **Blackbaud Users** who have **Privileged Accounts**, administrator accounts, and/or accounts, active or available, to design, maintain, operate, and update the **Blackbaud Network**.

h. Blackbaud shall implement and maintain controls to detect anomalous activity by unauthorized devices and prevent unauthorized devices from accessing the **Blackbaud Network**.

58. File Integrity Monitoring: Blackbaud shall maintain controls designed to provide near real-time notification of unauthorized or malicious modifications to **Blackbaud Customer** database servers in the **Blackbaud Network**. The notification shall include information available about the modification including, where available, the date of the modification, the source of the modification, the type of modification, and the method used to make the modification.

59. Unauthorized or Malicious Applications: Blackbaud shall maintain controls designed to identify and protect against the execution or installation of unauthorized or malicious applications on the **Blackbaud Network**.

60. Logging and Monitoring:

a. Within one hundred and eighty (180) days of the Effective Date, Blackbaud shall implement reasonable controls to centralize monitoring, logging, and operational activities on the **Blackbaud Network**; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance.

b. All **Security Incidents** shall promptly be reported to the **Chief Information Security Officer** and the Office of the **Chief Privacy Officer** consistent with the timeframes specified in the Blackbaud Incident Response Plan which, to the extent applicable, shall be aligned to NIST 800-61r2 and include processes for communicating **Security Incidents** to the appropriate leaders, executives, and committees to appropriately manage the risk. Any critical vulnerability that is associated with a **Security Incident** shall be remediated within twenty-four (24) hours of the identification of such vulnerability. If that vulnerability cannot be remediated as indicated above, then Blackbaud shall within twenty-four (24) hours of the identification of such vulnerability: (a) implement **Compensating Controls**; or (b) take the application or functionality of the application affected by such vulnerability offline until such vulnerability is remediated or **Compensating Controls** have been successfully applied.

c. Blackbaud shall monitor on a daily basis, and shall test on at least a monthly basis, any tool used to monitor the **Blackbaud Network** for the occurrence of a **Security Incident**, and properly configure, regularly update, and maintain the tool, so that the **Blackbaud Network** is appropriately monitored.

61. Change Control: Blackbaud shall maintain, regularly review and revise as necessary, and comply with a **Governance Process** established to manage and document changes to the **Blackbaud Network**. At a minimum:

a. Blackbaud shall define the roles and responsibilities for those involved in the change control process, including a board responsible for reviewing changes (hereinafter referred to as the "**Change Advisory Board**"). The **Change Advisory Board** shall include stakeholders from the appropriate business and informational technology units. The **Change Advisory Board**'s responsibilities shall include: managing overall change control policies and procedures; providing guidance regarding the overall change control policies and procedures; conducting an annual audit of change requests so that changes to the **Blackbaud Network** are properly analyzed and prioritized; and reviewing, approving, evaluating, and scheduling requests for changes to the **Blackbaud Network**.

b. The change control policies and procedures shall address the process to: request a change to the **Blackbaud Network**; determine the priority of the change; determine the change's impact on the **Blackbaud Network**, the security of **PI** and **PHI** on the **Blackbaud Network**, and Blackbaud's ongoing business operations; obtain the appropriate approvals from required personnel (e.g., change requester, area of Blackbaud business, **Change Advisory Board**); develop, test, and implement the

change; and review and test the impact of the change on the security of the **Blackbaud Network**, in each case as appropriate, based on the risk.

c. The change control policies and procedures required by this Paragraph shall require that any architectural changes to the **Blackbaud Network** be evaluated regarding potential risks, and that all such changes receive appropriate (i) analysis, (ii) approvals from required personnel, and (iii) testing, as appropriate, based on the risk.

d. Any action with respect to any changes to the **Blackbaud Network** (requesting, analyzing, approving, developing, implementing, and reviewing) shall be documented and retained, with the documentation appropriately secured and stored in repositories that are scoped to an application, area of Blackbaud business, and/or geography and are accessible to appropriate security personnel.

62. Asset Inventory: Blackbaud shall utilize processes and, where practicable, automated tool(s) to regularly inventory and classify, and issue reports on, all assets that comprise the **Blackbaud Network**. The asset inventory as well as applicable configuration and change management systems shall, at a minimum, collectively identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the **Blackbaud Network**; (e) the asset's criticality rating; (f) the potential risks and vulnerabilities associated with each asset; and (g) whether the asset processes or stores **PI** or **PHI** of **Consumers**. For purposes of this Paragraph, "assets" shall mean network components, data stores, physical devices, systems, software platforms, and applications within the **Blackbaud Network**. The requirements of this Paragraph shall commence upon one hundred and eighty (180) days after the Effective Date.

63. Digital Certificates: Blackbaud shall implement and maintain a **Governance Process** to manage the life cycle of all digital certificates that expire longer than a week after their creation and that are used to authenticate servers and systems in the **Blackbaud Network**, including whether to issue, cancel, renew, reissue, or revoke a digital certificate. The **Governance Process** required by this Paragraph shall track the expiration date of any such digital certificate and require notification of such expiration to the custodian of the certificate key thirty days (30) prior to expiration, ten days (10) prior to expiration, and on the date the digital certificate expires. Digital certificate for purposes of this Paragraph shall include a security token, biometric identifier, or a cryptographic key used to protect externally-facing systems and applications.

64. Endpoint Detection and Response ("EDR"): Blackbaud shall acquire, configure, and utilize, an EDR solution to incorporate real-time threat detection and analysis across the **Blackbaud Network** and Blackbaud owned and/or managed devices. Blackbaud shall operationally staff and manage such EDR solution with the necessary and qualified information security personnel and analyst technicians needed to operate and manage the solution. In addition to any in-house information security personnel and analyst technicians, Blackbaud shall also retain as part of any solution configuration, EDR solution professional services to assist with near real-time threat detection and monitoring.

65. Intrusion Detection and Prevention Tools ("IDS/IPS"): Blackbaud shall implement, maintain, and update intrusion detection and prevention tools including but not limited to host-based firewalls, antivirus/antimalware software, and logging on all internal servers and employee computers on the **Blackbaud Network** to detect and prevent malicious activity.

66. Threat Management: Blackbaud shall establish a threat management program which shall include the use of automated tools to continuously monitor the **Blackbaud Network**

for active threats. Blackbaud shall continuously monitor, and assess on at least a monthly basis, whether any monitoring tool used pursuant to this Paragraph is appropriately configured, tested, and updated.

67. Updates and Patch Management: Within one hundred and eighty (180) days of the Effective Date, Blackbaud shall maintain, keep updated, and support the software on the **Blackbaud Network**, taking into consideration the impact a software update will have on data security in the context of the **Blackbaud Network** and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. At a minimum, Blackbaud shall also do the following:

a. For any software that will no longer be supported by its manufacturer or a third party, Blackbaud shall commence the evaluation and planning to replace the software or to maintain the software with appropriate **Compensating Controls** the later of one (1) year prior to the date on which the manufacturer's or third party's support will cease, or ninety (90) days from the date the manufacturer or third party announces that it is no longer supporting the software if such period is less than one (1) year. If Blackbaud is unable to commence the evaluation and planning in the timeframe required by this subparagraph, it shall prepare and maintain a written exception that shall include:

i. A description of why the exception is appropriate, e.g., what business need or circumstance supports the exception;

ii. An assessment of the potential risk posed by the exception; and

iii. A description of the schedule that will be used to evaluate and plan for the replacement of the software or addition of any **Compensating Controls**.

b. Blackbaud shall maintain reasonable controls to address the potential impact security updates and security patches may have on the **Blackbaud Network** and shall:

i. Maintain a patch management solution(s) to manage software patches that includes the use of standardized patch management distribution tool(s), including automation-assisted processes, whenever appropriate; and

ii. Maintain a tool that includes an automated Common Vulnerabilities and Exposures (CVE) feed. The CVE tool required by this subparagraph shall provide Blackbaud regular updates, including daily updates to the extent available, regarding known CVEs for vendor-purchased software applications in use within the **Blackbaud Network**. Blackbaud may satisfy its obligations under this subparagraph by using an industry-standard vulnerability scanning tool. The CVE tool required by this subparagraph shall also:

a) Identify, confirm, and enhance discovery of the parts of the **Blackbaud Network** that may be subject to CVE events and/or incidents;

b) Scan the **Blackbaud Network** for CVEs; and

c) Scan the **Blackbaud Network** to determine whether scheduled security updates and patches have been successfully installed, including whether any security updates or patches rated as critical have been installed consistent with the requirement of this Assurance.

c. Blackbaud shall appoint one or more individuals responsible for patch management relating to the **Blackbaud Network** ("**Patch Management Group**") Blackbaud shall appoint one or more individuals who shall be responsible for overseeing the **Patch Management Group** ("**Patch Supervisor**"). The **Patch Supervisor** and the members of the **Patch Management Group** shall include persons with appropriate experience and qualifications. The **Patch Management Group** shall be responsible for:

   i. Monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from the tools installed pursuant to subparagraph (b) and completing appropriate and timely application of all relevant security updates and/or security patches;

   ii. Monitoring compliance with policies and procedures regarding ownership, supervision, evaluation, and coordination of the maintenance, management, and application of all security patches and software and application security updates by appropriate information technology (IT) application and system owners;

   iii. Supervising, evaluating, and coordinating any system patch management tool(s) such as those identified in subparagraph (b); and

   iv. A training requirement for individuals responsible for implementing and maintaining Blackbaud's patch management policies.

d. Blackbaud shall use the inventory created pursuant to Paragraph 62 in its regular operations to assist in identifying assets within the **Blackbaud Network** for purposes of applying security updates or security patches that have been released.

e. Blackbaud shall employ processes, procedures, and technology for the timely scheduling and installation of any security update and security patch relevant to the **Blackbaud Network.** Security update and security patch scheduling and installation shall be based upon priority of threat level, services storing **PI** and/or **PHI**, and public/external facing services that are processing **PI** and/or **PHI**. Blackbaud shall also consider NIST SP 800-40r4 ("Guide to Enterprise Patch Management Planning") and any relevant severity ratings, security alerts, and advisory notices disseminated by software and application vendors, the Cybersecurity and Infrastructure Security Agency (CISA), and/or an equivalent United States Department of Homeland Security (DHS) agency designated as responsible for cybersecurity. Blackbaud may adjust the severity rating of the security update or security patch using a risk-based approach that is documented with written explanation. If Blackbaud is unable to schedule and install the security update or security patch in accordance with the applicable severity or risk-based rating, Blackbaud shall identify the assets to which it applies, and create a written explanation that shall include:

i. A description of why the action is appropriate, e.g., what business need or circumstance exists that supports the rating;

ii. A description of the alternatives that were considered, and why they were not appropriate;

iii. An assessment of the potential risks posed by the action;

iv. The anticipated length of time for the action, if the action is temporary; and

v. To the extent applicable, a plan for managing or mitigating those risks identified in subparagraph (e)(iii) (e.g., **Compensating Controls**, alternative approaches, methods). The written explanation required by this subparagraph shall be prepared within forty-eight (48) hours of its determination to apply an exception.

f. Blackbaud shall, within a time period appropriate to the risk to the **Blackbaud Network**, but not later than forty-eight (48) hours of rating any security update or patch as critical or critical zero-day, either: (1) apply such update or patch to the **Blackbaud Network**; (2) apply **Compensating Controls**; or (3) if Blackbaud is unable to timely update or patch the **Blackbaud Network,** or apply **Compensating Controls,** Blackbaud will take the identified application or affected functionality of the identified application offline until the update or patch or **Compensating Controls** has been successfully applied. If Blackbaud chooses not to apply such update or patch to the **Blackbaud Network** and instead to implement **Compensating Controls**, it shall prepare and maintain a written exception that shall include:

i. A description of why the exception is appropriate, e.g., what business need or circumstance supports the exception;

ii. An assessment of the potential risk posed by the exception; and

iii. A description of the schedule that will be used to evaluate and plan for the application of the security update or patch or addition of any Compensating Controls.

g. In connection with the scheduling and installation of any critical patch and/or update, Blackbaud shall verify that the patch and/or update was applied and installed successfully throughout the **Blackbaud Network**. For each security update or security patch rated as critical, Blackbaud shall maintain records identifying: (1) each critical patch or update that has been applied; (2) the date(s) each patch or update was applied; (3) the assets to which each patch or update was applied; and (4) whether each patch or update was applied and installed successfully (the "**Critical Patch Management Records**"). Modifications to the **Critical Patch Management Records** shall be reviewed on a weekly basis by the **Patch Management Group**.

h. On a monthly basis, Blackbaud shall perform an internal assessment of its management and implementation of security updates and patches for the **Blackbaud Network**. This assessment shall identify (i) all known vulnerabilities to the **Blackbaud Network** and (ii) the updates or patches applied to address each vulnerability. The assessment will be formally identified, documented, and reviewed by the **Patch Management Group**.

68. Implementation Benchmarks: Blackbaud shall maintain a cybersecurity capability roadmap, conduct appropriate planning designed to assist Blackbaud in achieving the cybersecurity capabilities specified on the roadmap, and document progress and completion of projects establishing those cybersecurity capabilities.

H. ASSESSMENT AND REPORTING REQUIREMENTS

69. Third-Party Assessments of Information Security Program: Blackbaud shall engage an independent third party ("**Third-Party Assessor**") to conduct assessments of its general data

security practices, which includes a risk assessment that complies with **HIPAA**, as well as its compliance with the terms of this Assurance ("**Third-Party Assessments**"), as follows:

a. The **Third-Party Assessor** shall be a Certified Information Systems Security Professional (CISSP) or a Certified Information Systems Auditor (CISA), or a similarly qualified person or organization and have at least three (3) years of experience evaluating the effectiveness of computer system security or information system security.

b. The reporting period for the **Third-Party Assessments** must cover: (1) the first one hundred and eighty (180) days after the **Effective Date** for the initial **Third-Party Assessment**; and (2) every other year thereafter for seven (7) years, for a total of four (4) **Third-Party Assessments** completed in the first, third, fifth, and seventh years after the **Effective Date**.

c. The **Third-Party Assessments** shall:

   i. Follow a NIST Cybersecurity Framework or another established industry standard cybersecurity framework;

   ii. Identify the specific administrative, technical, and physical safeguards maintained by Blackbaud's **Information Security Program**;

   iii. Document the extent to which the identified administrative, technical and physical safeguards are appropriate considering Blackbaud's size and complexity, the nature and scope of Blackbaud's activities, and the sensitivity of the **PI** and **PHI** maintained on the **Blackbaud Network**; and

iv. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Blackbaud meet the requirements of the **Information Security Program** and **HIPAA**.

d. Following each such assessment, the **Third-Party Assessor** shall prepare a report including its findings and recommendations to cover the requirements under subparagraphs 69(c)(i)-(iv) ("**Security Report**") and provide a copy of the **Security Report** to Blackbaud. A copy of the **Security Report** shall be provided to the Indiana Attorney General within thirty (30) days of the completion of the **Security Report**. The Indiana Attorney General may provide a copy of the **Security Report** to the states identified in Footnote 2 upon request.

e. Within ninety (90) days of its receipt of each **Security Report**, Blackbaud shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the **Security Report**. Within one hundred eighty (180) days of Blackbaud's receipt of each **Security Report**, Blackbaud shall forward to the Indiana Attorney General a description of any action they take and, if no action is taken, a detailed description of why no action is necessary, in response to each **Security Report**. The Indiana Attorney General may provide a copy of Blackbaud's response as indicated in the foregoing sentence to each **Security Report** to the states identified in Footnote 2 upon request.

f. Any **Security Report** provided pursuant to this Paragraph and all information contained therein, to the extent permitted by the laws of Maryland: shall be treated by the Division as confidential; shall not be shared or disclosed except as permitted by subpart (d) of this Paragraph; and shall be treated by the Division as exempt from disclosure under the relevant public records laws of Maryland. In the event that the

Division receives any request from the public for any **Security Report** provided pursuant to this Paragraph or other confidential documents provided to the Division under this Assurance, and believes that such information is subject to disclosure under the relevant public records laws, the Division agrees to provide Blackbaud with at least ten (10) days advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that Blackbaud may take appropriate action to defend against the disclosure of such information. The notice under this Paragraph shall be provided consistent with the notice requirements contained in Paragraph 92. Nothing contained in this subparagraph shall alter or limit the obligations of the Division that may be imposed by the relevant public records laws of the State of Maryland, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to the Division except with respect to the obligation to notify Blackbaud of any potential disclosure.

70. In the event that any audit or other third-party report pertaining to cybersecurity is materially amended or withdrawn, Blackbaud shall immediately notify any **Blackbaud Customer** or governmental agency with which it has shared the report.

V. DOCUMENT RETENTION

71. Unless otherwise provided herein, Blackbaud shall retain and maintain any documentation required by Paragraphs 12 and 31-70 for a period of no less than seven (7) years. In no way does this or any other provision in this Assurance waive any applicable privilege or protection over any Blackbaud document or communication.

VI. PAYMENT TO THE STATES

72. Within thirty (30) days of the **Effective Date**, Blackbaud shall pay a total of Forty-Nine Million, Five Hundred Thousand Dollars ($49,500,000) to the Attorneys General, to be

divided among the Attorneys General at their discretion. The amount apportioned to the Division is to be paid by Blackbaud directly to the Division in an amount designated by the Attorneys General and communicated to Blackbaud.

73. Out of the total amount, Blackbaud shall pay $820,156 to the Division. The money received by the Division pursuant to this section may be used, at the sole discretion of the Attorney General, for purposes that may include placement in any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, or litigation, used to defray the costs of the inquiry leading hereto, or may be used for any other public purpose permitted by state law.

VII. RELEASE

74. Following full payment of the amounts due under this Assurance, the Division shall release and discharge Blackbaud from all civil or administrative claims that the Division could have brought under the **Relevant Laws** based on Blackbaud's conduct related to the **2020 Data Breach**. Nothing contained in this Paragraph shall be construed to limit the ability of the Division to enforce the obligations that Blackbaud has under this Assurance. Further, nothing in this Assurance shall be construed to (a) create, waive, or limit any private right of action; or (b) excuse or exempt Blackbaud from complying with any state or federal law, rule, or regulation in the future. For clarity, the execution of this Assurance terminates the tolling agreement between Blackbaud and the Division.

75. Notwithstanding any term of this Assurance, any and all of the following forms of liability are specifically excluded from the release in Paragraph 74 above as to any entity or person, including Blackbaud:

a. Any criminal liability that any person or entity, including Blackbaud, has or may

have to the States; and

b. Any civil liability or administrative liability that any person or entity, including Blackbaud, has or may have to the States under any statute, regulation, or rule not expressly covered by the release in Paragraph 74 above, including but not limited to, any and all of the following claims: (i) State or federal antitrust violations; (ii) State or federal securities violations; (iii) State insurance law violations; or (iv) State or federal tax claims.

76. This Assurance is not intended, and shall not be deemed, to constitute evidence or precedent of any kind except in: (a) any action or proceeding by one of the Parties to enforce, rescind, or otherwise implement or affirm any or all terms of this Assurance; or (b) any action or proceeding involving a claim covered by the release to support a defense of res judicata, collateral estoppel, release or other theory of claim preclusion, issue preclusion, or similar defense.

VIII. GENERAL PROVISIONS

77. Nothing in this Assurance shall be construed to limit the authority or ability of the Division to protect the interests of Maryland or the people of Maryland. This Assurance shall not bar the Division or any other governmental entity from enforcing laws, regulations, or rules against Blackbaud for conduct subsequent to or otherwise not covered by this Assurance. Further, nothing in this Assurance shall be construed to limit the ability of the Division to enforce the obligations that Blackbaud has under this Assurance.

78. The requirements of the Assurance are in addition to, and not in lieu of, any other requirements of state or federal law. Nothing in this Assurance shall be construed as relieving Blackbaud of the obligation to comply with all state and federal laws, rules, and regulations, nor shall any of the provisions of this Assurance be deemed to be permission to engage in any acts or

practices prohibited by such laws, rules, and regulations.

79. Any failure of the Division to exercise any of its rights under this Assurance shall not constitute a waiver of any rights hereunder.

80. The Parties agree that should Blackbaud resolve allegations concerning Blackbaud's conduct related to the **2020 Data Breach** with Attorneys General of other States and, within sixty (60) days, if the Division determines that the injunctive terms of such resolution(s), taken as a whole, are materially more favorable than those contained in this Assurance, then the Division shall notify Blackbaud in writing within fifteen (15) days regarding its position that another State's terms are materially more favorable and the Division and Blackbaud shall meet and confer regarding whether and how favorable the injunctive terms of such resolution(s) are compared to those contained in this Assurance. Within ten (10) days after the meet and confer, Blackbaud shall notify the Division in writing whether it, in whole or in part, agrees with the Division's proposal or contests the applicability of this provision in good faith. The Parties shall promptly commence negotiation over the relevant terms. Once the Division and Blackbaud have mutually agreed that certain injunctive terms of such resolution are materially more favorable than those contained in this Assurance, this Assurance shall be amended accordingly. This Paragraph shall expire one (1) year after the Effective Date. Notwithstanding the foregoing, this Paragraph shall not apply to the differences in resolutions with the States that have agreed to this Assurance as part of the multi-state.

81. Nothing contained in this Assurance is intended to be, and shall not in any event be construed or deemed to be, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Blackbaud or of any fact or violation of law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any

finding of liability or wrongdoing of any kind. Blackbaud enters into this Assurance for settlement purposes only.

82. Blackbaud shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Assurance or for any other purpose that would otherwise circumvent any term of this Assurance. Blackbaud shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Assurance.

83. In states where this Assurance must be filed with and/or approved by a court, Blackbaud consents to the filing of this Assurance and its approval by the court, and authorizes the Attorneys General in such states to represent that Blackbaud does not object to court approval of the Assurance. Blackbaud further consents to the jurisdiction of each such court for the purpose of approving, modifying, or enforcing the Assurance. Blackbaud shall pay all court costs associated with the filing of this Assurance, as applicable.

84. Blackbaud agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees under any statute, regulation, or rule, and Blackbaud further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

85. This Assurance shall not be construed to waive any claims of sovereign immunity that Maryland may have in any action or proceeding.

86. Blackbaud shall deliver a copy of this Assurance to, and otherwise fully apprise, its Chief Executive Officer, General Counsel, **Chief Privacy Officer**, **Chief Information Security Officer**, **Business Information Security Officers, Chief Technology Officer,** and Board of Directors within thirty (30) days of the **Effective Date**. To the extent Blackbaud replaces any of the above-listed officers, counsel, or directors, Blackbaud shall deliver a copy of this Assurance to

their replacements within thirty (30) days from the date on which such person assumes his or her position with Blackbaud.

87. If any portion of this Assurance is held invalid or unenforceable, the remaining terms of this Assurance shall not be affected and shall remain in full force and effect.

88. No modification of the terms of this Assurance shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Assurance is filed, as applicable, and then only to the extent specifically set forth in such Assurance. However, the Parties may agree in writing, through counsel, to an extension of any time period specified in this Assurance without a court order.

89. Nothing in this Assurance shall provide any rights to or permit any person or entity not a party hereto, including any state or attorney general not a party hereto, to enforce any provision of this Assurance. No person or entity not a signatory hereto is a third-party beneficiary of this Assurance. Nothing in this Assurance shall be construed to create, affect, alter, or assist any private right of action that a **Consumer** or other third-party may hold against Blackbaud.

90. The Parties hereby acknowledge that their undersigned representative or representatives are authorized to enter into and execute this Assurance. Blackbaud is and has been represented by legal counsel and has been advised by its legal counsel of the meaning and legal effect of this Assurance.

91. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Assurance may be executed in counterparts, each of which shall be deemed an original, but all of which shall be considered one and the same Assurance.

IX. NOTICES

92. Any notices or other documents required to be sent to the Parties pursuant to the

Assurance shall be sent by United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. Any notices or other documents sent pursuant to the Assurance shall be sent to:

For the Division:

Hanna Abrams
Assistant Attorney General
Consumer Protection Division
Office of the Attorney General
200 St. Paul Place, 16th Floor
Baltimore, MD 21202

Chief
Consumer Protection Division
Office of the Attorney General
200 St. Paul Place, 16th Floor
Baltimore, MD 21202

For BLACKBAUD:

Robert J. Mittman
1271 Avenue of the Americas
New York, NY 10020

Sharon R. Klein
4 Park Plaza, Suite 450
Irvine, CA 92614

Paul H. Tzur
444 West Lake Street, Suite 1650
Chicago, IL 60606

A Party may update its designee or address by sending written notice to the other Party informing them of the change.

APPROVED:

FOR THE CONSUMER PROTECTION DIVISION OF THE OFFICE OF THE ATTORNEY GENERAL OF MARYLAND:

ANTHONY G. BROWN
ATTORNEY GENERAL OF MARYLAND

By: _____ Date: 10/5/2023
William D. Gruhn
Chief
Consumer Protection Division
Office of the Attorney General of Maryland

By: _____ Date: 10/5/23
Hanna Abrams
Assistant Attorney General
Consumer Protection Division
Office of the Attorney General of Maryland
200 Saint Paul Place, Baltimore, MD 21202

[Additional approvals on subsequent pages]

APPROVED:

BLACKBAUD, INC.

By: _____

Name: Anthony W. Boor

Title: Chief Financial Officer

Date: 9/25/2023

APPROVED:

COUNSEL FOR BLACKBAUD, INC.
BLANK ROME, LLP

By: _____

Name: Robert J. Mittman

Title: Partner

Date: 9/25/2023

BLACKBAUD MULTISTATE APPENDIX - EXHIBIT A

STATE	CONSUMER PROTECTION LAWS	DATA BREACH NOTIFICATION & PERSONAL INFORMATION PROTECTION LAWS
AK - ALASKA	Unfair Trade Practices Act, Alaska Stat. 45.50.471, et seq.	Alaska Stat. 45.48.010, et seq.
AL - ALABAMA	Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-1, et seq.	Data Breach Notification Act of 2018, Ala. Code § 8-38-1, et seq.
AR - ARKANSAS	Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101, et seq.	Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-101, et seq.
AZ - ARIZONA	Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, et seq.	Ariz. Rev. Stat. §§ 18-551 and 18-552
CO - COLORADO	Colorado Consumer Protection Act, C.R.S. §§ 6-1-101 et seq.	C.R.S. § 6-1-716 and C.R.S. § 6-1-713.5
CT- CONNECTICUT	Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b, et seq.	Breach of Security, Conn. Gen. Stat. § 36a-701b; Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
DC - DISTRICT OF COLUMBIA	Consumer Protection Procedures Act, D.C. Code §§ 28-3901, et seq.	District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, et seq.
DE - DELAWARE	Consumer Fraud Act, 6 Del. C. §§ 2511 et seq.	Delaware Data Breach Notification Law, 6 Del. C. § 12B-100 et seq.
FL - FLORIDA	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes	Florida Information Protection Act, Section 501.171, Florida Statutes
GA - GEORGIA	Georgia Fair Business Practices Act, O.C.G.A. §§ 10-1-390 through 408	Georgia Personal Identity Protection Act, O.C.G.A §§ 10-1-910 through 915
HI - HAWAII	Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. ch. 481A and Haw. Rev. Stat. § 480-2	Haw. Rev. Stat. ch. 487J and Haw. Rev. Stat. ch. 487N
IA - IOWA	Iowa Consumer Fraud Act, Iowa Code § 714.16	Personal Information Security Breach Protection Act, Iowa Code Chapter 715C
ID - IDAHO	Idaho Consumer Protection Act, Idaho Code §§ 48-601, et seq.	Idaho Code, Title 28, Chapter 51
IL - ILLINOIS	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 et seq.	Illinois Personal Information Protection Act, 815 ILCS 530/1 et seq.
IN - INDIANA	Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5 et seq.	Disclosure of Security Breach Act, Ind. Code §§ 24-4.9 et seq.
KS - KANSAS	Kansas Consumer Protection Act, K.S.A §§ 50-623 et seq.	Security Breach Notification Act, K.S.A. §§ 50-7a01, et seq.; The Wayne Owen Act, K.S.A. § 50-6,139b

BLACKBAUD MULTISTATE APPENDIX - EXHIBIT A

KY - KENTUCKY	Kentucky Consumer Protection Act, KRS §§ 367.110-.300, 367.990	KRS 365.732
LA - LOUISIANA	Unfair Trade Practices and Consumer Protection Law, La. R.S. §§ 51:1401, et seq.	Database Security Breach Notification Law, La. R.S. §§ 51:3071, et seq.
MA - MASSACHUSETTS	Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A	Mass. Gen. Laws ch. 93H; 201 Code Mass. Regs. 17.00 et seq.
MD - MARYLAND	Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101, et seq.	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501, et seq.
ME - MAINE	Maine Unfair Trade Practices Act, 5 M.R.S.A. §§ 205-A, et seq.	Maine Notice of Risk to Personal Data Act, 10 M.R.S.A. §§ 1346, et seq.
MI - MICHIGAN	Michigan Consumer Protection Act, MCL 445.901 et seq.	Identity Theft Protection Act, MCL 445.61, et seq.
MN - MINNESOTA	Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43–.48; Consumer Fraud Act, Minn. Stat. §§ 325F.68-.694	Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61 and Minnesota Health Records Act, Minn. Stat. § 144.291-144.34
MO - MISSOURI	Mo. Rev. Stat. §§ 407.010, et seq.	Mo. Rev. Stat. § 407.1500
MS - MISSISSIPPI	Mississippi Consumer Protection Act, Miss. Code §§ 75-24-1, et seq.	Miss. Code Ann. § 75-24-29
MT - MONTANA	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. §§ 30-14-101 et seq.	Mont. Code Ann. §§ 30-14-1701 et seq.
NC - NORTH CAROLINA	North Carolina Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1, et seq.	Identity Theft Protection Act, N.C.G.S. §§ 75-60, et seq.
ND - NORTH DAKOTA	Unlawful Sales or Advertising Practices, N.D.C.C. §§ 51-15-01 et seq.	Notice of Security Breach for Personal Information N.D.C.C. §§ 51-30-01 et seq.
NE - NEBRASKA	Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601 et seq.	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 et seq.
NH - NEW HAMPSHIRE	New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann § 358-A:1, et seq.	N.H. Rev. Stat. Ann § 359-C: 19-21
NJ - NEW JERSEY	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq.	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
NM - NEW MEXICO	New Mexico Unfair Practices Act, NMSA 1978, §§ 57-12-1 et seq.	Data Breach Notifications Act, NMSA 1978, Sections 57-12C-1 et seq.

BLACKBAUD MULTISTATE APPENDIX - EXHIBIT A

NV - NEVADA	Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903 et seq.	Nev. Rev. Stat. §§ 603A.010-603A.290
NY - NEW YORK	Executive Law 63(12), General Business Law 349/350	General Business Law 899-aa and 899-bb
OH - OHIO	Ohio Consumer Sales Practices Act, R.C. § 1345.01, et seq.	R.C. § 1349.19, et seq.
OK - OKLAHOMA	Oklahoma Consumer Protection Act, 15 O.S. Section 751, et seq.	Oklahoma Security Breach Notification Act, 24 O.S. Section 161, et seq.
OR - OREGON	Oregon Unlawful Trade Practices Act, ORS 646.605, et seq.	Oregon Consumer Information Protection Act, ORS 646A.600, et seq.
PA - PENNSYLVANIA	Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, et seq.	Breach of Personal Information Notification Act, 73 P.S. §§ 2301, et seq.
RI - RHODE ISLAND	Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1, et seq.	Rhode Island Identity Theft Protection Act R.I. Gen. Laws §§ 11-49.3-1, et seq.
SC - SOUTH CAROLINA	South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10, et seq.	South Carolina Data Breach Notification Law, S.C. Code Ann. § 39-1-90
SD - SOUTH DAKOTA	SDCL Chapter 37-24	SDCL Chapter 22-40
TN - TENNESSEE	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -135	Tennessee Identify Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 to -2111
TX - TEXAS	Texas Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann. §§ 17.41 – 17.63	Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521.001 – 152
UT - UTAH	Utah Consumer Sales Practices Act Utah Code §§ 13-11-1, et. seq.	Utah Protection of Personal Information Act, Utah Code §§ 13-44-101, et seq.
VA - VIRGINIA	Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207	Virginia Breach of Personal Information Notification Law, Virginia Code § 18.2-186.6
VT - VERMONT	Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 et seq.	9 V.S.A §§ 2430, 2431, and 2435
WA - WASHINGTON	Washington Consumer Protection Act, RCW 19.86 et seq.	Washington Data Breach Notification Law, RCW 19.255 et seq.
WI - WISCONSIN	Wis. Stat. § 100.18(1)	Wis. Stat. § 134.98
WV - WEST VIRGINIA	W. Va. Code §§ 46A-1-101, et seq.	W. Va. Code §§ 46A-2A-101 et seq.
WY - WYOMING	Wyoming Consumer Protection Act, W.S. §§ 40-12-101 et seq.	W.S. §§ 40-12-501 et seq.