Data Security Addendum

1. **Information Security Measures and Governance Commitment.** Blackbaud will maintain, while it processes Client Data, technical and organizational measures designed to safeguard Client Data in accordance with this Addendum and applicable laws. Blackbaud will maintain a cybersecurity and risk management program ("Cybersecurity Program") designed to preserve the confidentiality, integrity and accessibility of Client Data with administrative, technical, procedural and physical measures conforming to generally recognized industry standards, including, as applicable and as made part of the Cybersecurity Program: Payment Card Industry Data Security Standard (PCI DSS), International Standards Organization (ISO)/IEC 27001, Informative References within the United States Cybersecurity Framework, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Blackbaud will refrain from making any changes to the Cybersecurity Program or specific safeguards that materially reduce the level of security provided to Client Data. Blackbaud will maintain documentation that describes in detail the Cybersecurity Program.

2. **Definitions.**

   a. "Client Data" will mean Client Data or "Your Data" as defined in the Agreement, and if no such definition is found in the Agreement, Client Data as used herein will mean Client's Confidential Information, all Client data provided to Blackbaud for processing, including personal data or personal information (or other analogous terms) as defined under relevant privacy and data protection laws, and any artwork, logos, trade names, and trademarks that Client provides to Blackbaud.

   b. "Client's Confidential Information" for the purposes of the definition of Client Data above, will mean Confidential Information as defined in the Agreement, and if no such definition is found in the Agreement, Client's Confidential Information as used herein will mean (i) all information disclosed by Client to Blackbaud electronically, visually, orally or in a tangible form which is either (a) marked as "confidential" (or with a similar legend), (b) is identified at the time of disclosure as being confidential, or (c) should be reasonably understood to be confidential or proprietary; and (ii) donor, student, employee, prospect information, and financial information of any of the foregoing.

   c. "Solutions" means Subscriptions and Services collectively, as defined in the Agreement, and if no such definition is found in the Agreement, "Solution" will mean Blackbaud's Software as a Service Application provided to Client under the Agreement, which includes Blackbaud's computing environment in which the Solution is installed and maintained.

3. **Cybersecurity Program - Detailed Technical and Organizational Security Measures**.

   a. **Network Security**. Blackbaud agrees to maintain security measures for its network, including, as applicable and made part of the Cybersecurity Program: endpoint security, network security protocols, network identification services, data encryption, integrity that includes industry standard firewall protection, intrusion detection services and intrusion prevent systems, data availability safeguards (back-ups, redundancy mechanisms), reliable and interoperable security processes and periodic vulnerability scans for the relevant Solutions.

   b. **Security Updates and Patching.** Blackbaud's update and patching program is focused on maintaining the hosting infrastructure with up-to-date patches and all appropriate security updates as designated by the relevant manufacturer or authority (e.g. Microsoft notifications) and to keep the hosting infrastructure free of known viruses, worms, spyware, adware, malware, and other malicious and unwanted software and programs. Blackbaud has a Change Management Board ("CMB"), for patch management and updates. The

CMB consists of members of the Engineering, Development, and Security departments, and meets regularly to plan, review, and approve changes to hardware, software, operating systems, and Solutions.

c. **Software Development Security.** Blackbaud Solutions are developed using industry standard best practices throughout the Software Development Life Cycle. Blackbaud's development teams use a secure software development methodology for guiding their planning and process management and leverage industry standards and best practices for secure coding, such as the Open Web Application Security Project (OWASP) "Top 10" list for secure coding practices. All Solutions undergo stringent quality assurance testing before being deployed to Blackbaud's production environment. Blackbaud will use commercially reasonable efforts to regularly identify software vulnerabilities and, in the case of known software vulnerabilities, to provide relevant updates, upgrades, and bug fixes for Solutions.

d. **Independent security assessments**.
   i. Vulnerability testing - Blackbaud has a comprehensive vulnerability management program. All of Blackbaud's Solutions and Blackbaud's public facing infrastructure go through annual third-party penetration testing. Blackbaud also performs its own internal and external vulnerability scans on a quarterly basis, as well as static code scans against Solutions during key moments in the development lifecycle. Any issues found are submitted for remediation based on industry recommendations.
   ii. Blackbaud leverages relevant industry frameworks, such as the Control Objectives for Information and Related Technology (COBIT) framework in alignment with Sarbanes-Oxley ("SOX"), external SOX audits are performed annually and relevant findings from such audit are provided in Blackbaud's public (e.g. SEC) filings.
   iii. Security audit - Blackbaud has an annual American Institute of Certified Public Accountants Service Organization Control ("SOC") audit conducted for the Security Trust Principle, and will provide to Company upon request, once annually, a copy of the resulting SOC audit report.

e. **Strong Authentication**. Blackbaud will enforce strong authentication for any: i) remote access to Client Data; and ii) administrative and/or management access to Blackbaud security infrastructure and Blackbaud log data.

f. **Physical and Environmental Security**. Blackbaud enforces physical datacenter security based on best practices and SSAE18 audit guidelines, including the following:
   i. All building entrances, the datacenter floor, and secure areas require access controls, such as card keys and in appropriate areas, two-factor biometric authentication.
   ii. Security is provided for the interior and exterior of Blackbaud's facilities, including, as appropriate, active patrol guards. Security cameras are in place covering all appropriate areas.
   iii. Blackbaud's datacenters provide industry standard power management, heating/ventilation/air conditioning (HVAC), fire detection and suppression, continuous monitoring, and access to intelligent IP networks.
   iv. 100% redundant power to provide the Client with continuous run time on full load during a disaster.

g. **Personnel confidentiality**: Blackbaud will ensure that any person that Blackbaud authorizes to process Client Data (including Blackbaud staff, agents and subcontractors, "Personnel") will be subject to an appropriate duty of confidentiality (whether contractual or statutory).

h. **Cybersecurity Awareness and Training**: Blackbaud will provide its Personnel with information security training upon hire and at least annually thereafter. Additionally, Blackbaud will use written acceptance of codes of conduct, ethics policies, or confidentiality agreements, to promote Personnel awareness and compliance with Blackbaud's information security policies and procedures. Blackbaud will maintain Personnel completion reports. Blackbaud will review the contents of its security awareness and training program at least annually to ensure it is updated to reflect current, relevant security information.

i. **Contingency Planning/ Incident Response Plan**: Blackbaud will have policies and procedures for responding to emergencies, cybersecurity incidents and other events that could damage or remove access to Client Data. Blackbaud maintains a proactive and protective information security incident response program aligned with industry standard practices to identify, contain, eradicate, and recover from security incidents. The program is consistently reviewed and tested with table-top exercises to simulate potential attacks and response scenarios to evaluate the program and stay vigilant against cyber-attacks.

j. **Storage and Transmission Security**: Blackbaud will have security measures to guard against unauthorized access to Client Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Client Data stored on desktops, laptops and tablets as applicable. Blackbaud does not permit any storage of Client Data on other mobile devices (e.g. mobile phones) or removable storage media.

k. **Secure Disposal:** Blackbaud maintains policies and procedures, aligned to NIST-800-88, regarding the secure disposal of media containing Client Data, considering available technology, so that Client Data cannot be practicably read or reconstructed.

l. **Monitoring and Logging**. Blackbaud will have intrusion detection systems, audit trail logging, and security event detection and monitoring in place for networks, servers, and applications where Client Data is stored, processed, or transmitted. Blackbaud will log and maintain for 12 months all physical and logical access to Client Data.

m. **Passwords:** When passwords are used to access Client Data, Blackbaud will enforce strong authentication in all instances. Where practicable, Blackbaud will use a second authentication factor before granting access to Client Data with a password.

    i. Passwords must be complex and meet relevant industry frameworks, including requirements for:
        1. minimum length.
        2. Including characters of different types: alpha, numeric, and special characters.
        3. Not be the same as the UserID with which they are associated.
    ii. Require password expiration at regular intervals in accordance with relevant industry frameworks.
    iii. When providing users with a new or reset password, or other authentication credentials, use a secure method to provide this information and maintain a written policy requiring reset at first login whenever a temporary credential is used.

n. **Encryption:** Blackbaud uses various strong encryption mechanisms across its environments and solutions to protect Client Data, which are in alignment with industry standard encryption algorithms. Blackbaud manages all secure communication configurations between its cloud solutions and its customers through the public key Infrastructure (PKI). Blackbaud use encrypted key vaults to hold keys.

o. **Access Management; Least privilege**: Blackbaud maintains formal processes to grant, prevent and terminate access to Client Data. Access is limited to users who require such access to perform their job responsibilities.

Blackbaud maintains a "least privilege" approach to access control. Only authenticated users with a business justification have access to production systems and Client Data. Internally, Blackbaud uses MFA for all employees with regular "challenge" requests to re-authenticate all sessions once a week. The creation and rotation of strong authentication credentials are enforced globally, and Blackbaud's access control policies enforce standard best practices around session-timeouts, maximum failed authentication attempts and password rotation.

p. **PCI DSS**. Blackbaud has validated and maintains compliance with the Payment Card Industry Data Security Standard ("PCI-DSS") and the Payment Application Data Security Standard ("PA-DSS") for each application that processes, stores, and transmits cardholder data as defined under the PCI-DSS. Blackbaud has implemented PCI standards regarding secure storage of data, strong access controls, and other requirements. Client may request a copy of Blackbaud's PCI Attestation of Compliance on an annual basis.