TRINITY UNIVERSITY
CONFIDENTIALITY and NON-DISCLOSURE AGREEMENT

THIS AGREEMENT is made by and between Trinity University (hereinafter the "UNIVERSITY") and _____ (hereinafter the "SERVICE PROVIDER"). This Agreement is applicable to SERVICE PROVIDER'S employees, subcontractors, vendors, agents, and other project participants.

WHEREAS, the UNIVERSITY anticipates that the Services of the SERVICE PROVIDER will be necessary and desirable; and

WHEREAS, the SERVICE PROVIDER desires to enter into an agreement with the UNIVERSITY to provide Services as described under the Services Contract between Trinity University and the SERVICE PROVIDER.

NOW THEREFORE, it is agreed as follows:

I. PROVISIONS CONCERNING CONFIDENTIAL INFORMATION

For the purposes of this Agreement, the term SERVICE PROVIDER shall include: SERVICE PROVIDER'S employees, subcontractors, vendors, agents, or other anticipated project participants. The term SERVICE PROVIDER shall be construed to mean those individuals who have a legitimate need to know the information being disclosed. This Agreement covers Confidential Information, which may include but is not limited to:

1. Confidential Information

Confidential Information is information that would be reasonably understood as confidential or proprietary or is designated as such in writing and includes, but is not limited to: confidential personnel information; private health information; student academic information; student financial information (including addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers); information pertaining to the UNIVERSITY's operations (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, etc.); credit card information received in the course of business by the UNIVERSITY; information pertaining to third parties who work with or on behalf of the UNIVERSITY (such as computer programs, client and vendor proprietary information, source code, proprietary technology, etc.); and all other Confidential Information referenced in this Section I.

2. Covered Data and Information

Covered Data and Information includes Student Financial Information (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as any credit card information received in the course of business by the UNIVERSITY, whether or not such credit card information is covered by GLB; education records (defined below) protected under the Family Educational Rights and Privacy Act (FERPA); and personal data (defined below) protected under EU GDPR. Covered data and information includes both paper and electronic records.

3. Student Financial Information

Student Financial Information is information that the UNIVERSITY has obtained from a customer in the process of offering a financial product or service, or such information provided to the UNIVERSITY by another financial UNIVERSITY. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 C.F.R. § 225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit

histories and Social Security numbers, in both paper and electronic format.

4. Education Records

Education Records include records containing any "personally identifiable information" from student education records as defined by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and the implementing regulations in Title 34, Part 99 of the Code of Federal Regulations ("FERPA").

5. Personal Data

Defined under the European Union's General Data Protection Regulation as any information relating to an identified or identifiable natural person (data subject) to include online identifiers and location data as well as reference to genetic factors.

6. Exceptions

The foregoing restrictions shall not apply to information that the SERVICE PROVIDER can demonstrate (1) was generally known prior to the date of disclosure of the same to the SERVICE PROVIDER by the UNIVERSITY; (2) was in the SERVICE PROVIDER's possession prior to the date of disclosure of the same to the SERVICE PROVIDER by the UNIVERSITY; (3) becomes generally known through no act or omission by the SERVICE PROVIDER; (4) is supplied to the SERVICE PROVIDER, subsequent to the date of disclosure of the same to the SERVICE PROVIDER by the UNIVERSITY, by a third party not under an obligation of confidentiality with respect to such information; or (5) is required to be disclosed by law or pursuant to an order of a court or other governmental agency of competent jurisdiction, in which case the SERVICE PROVIDER shall promptly notify the UNIVERSITY of such requirement to afford the UNIVERSITY an opportunity to prevent or limit such disclosure.

II. GENERAL OBLIGATIONS

As a SERVICE PROVIDER with access to Confidential Information, the SERVICE PROVIDER is required to conduct itself in strict conformance with applicable federal and state laws as well as the European Union's General Data Protection Regulation and UNIVERSITY's policies governing Confidential Information. The SERVICE PROVIDER's principal obligations in this area are explained below. The SERVICE PROVIDER is required to read and adhere to the obligations and duties established below or in the future by the UNIVERSITY as they relate to Confidential Information. The violation of any of these duties could result in revocation of access rights, severance of the contract and to legal liability arising from the UNIVERSITY or third parties.

The SERVICE PROVIDER hereby agrees and accepts the following obligations/duties as a condition of and in consideration of its access to Confidential Information;

a. The SERVICE PROVIDER will use Confidential Information only as needed to perform the specific functions assigned to the SERVICE PROVIDER.

b. The SERVICE PROVIDER will only access Confidential Information for which it has a need-to-know basis based upon its role;

c. The SERVICE PROVIDER will not in any way divulge, copy, release, sell, loan, review, alter or destroy any Confidential Information except as properly authorized within the scope of the SERVICE PROVIDER's role; and

d. The SERVICE PROVIDER will not misuse Confidential Information or carelessly handle Confidential Information.

III. COMPLIANCE WITH FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

In addition to the foregoing obligations, if UNIVERSITY provides SERVICE PROVIDER with any legally confidential information including but not limited to confidential personnel information or "personally identifiable information" from student education records as defined by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, and the implementing regulations in Title 34, Part 99 of the Code of Federal Regulations ("FERPA"), SERVICE PROVIDER hereby certifies that collection of this information from UNIVERSITY is necessary for the performance of the SERVICE PROVIDER'S duties and responsibilities on behalf of UNIVERSITY under this Agreement. SERVICE PROVIDER further agrees to handle information protected by FERPA in the manner set forth below.

SERVICE PROVIDER acknowledges that certain information about the UNIVERSITY's student(s) may be shared in conjunction with the activities performed under this Agreement and that this information is protected by the Family and Educational Rights and Privacy Act of 1974 (20 U.S. C. 1232g). To the extent that SERVICE PROVIDER has access to "education records" under this contract, it is deemed a "school official," as each of these term are defined under FERPA. SERVICE PROVIDER agrees that it shall not use education records for any purpose other than in the performance of this contract. Except as required by law, SERVICE PROVIDER shall not disclose or share education records with any third party unless permitted by the terms of this Agreement. Nothing contained herein precludes the parties from sharing information with one another so that each can perform its respective responsibilities.

IV. COMPLIANCE WITH GRAMM LEACH BLILEY ACT

SERVICE PROVIDER acknowledges that this Agreement may allow SERVICE PROVIDER access to Covered Data and Information as defined above. SERVICE PROVIDER agrees that such Covered Data and Information will be handled in the manner set forth below.

V. COMPLIANCE WITH EUROPEAN UNION GENERAL DATA PROTECTION REGULATIONS

SERVICE PROVIDER acknowledges that this Agreement may allow SERVICE PROVIDER to process Personal Data. In compliance with the European Union's General Data Protection Regulation, SERVICE PROVIDER agrees to adhere to the confidentiality expectations as outlined in the EU General Data Protection Regulation (GDPR) and require the same of any subcontractors that perform services in concurrence with this Agreement.

VI. MISCELLANEOUS

A. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information

The SERVICE PROVIDER agrees to hold the Confidential Information in strict confidence. The SERVICE PROVIDER shall not use or disclose Confidential Information received from or on behalf of the UNIVERSITY except as permitted or required by the Service Contract or this Agreement, as required by law, or as otherwise authorized in writing by the UNIVERSITY.

B. Safeguard Standard

The SERVICE PROVIDER agrees that it will protect the Confidential Information that it receives from or on behalf of the UNIVERSITY according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

For any individuals who will have access to financial information, social security numbers, confidential or proprietary information, as determined by Trinity University, a criminal background check is required. A credit history report is also required for individuals who may be assigned to finance and accounting

positions. Any individuals who have criminal or civil convictions related to financial wrongdoing including, but not limited to, embezzlement, fraud, money laundering, theft or other acts indicating dishonesty may not be assigned to Trinity University if such assignment would involve access to financial information, social security numbers, confidential or proprietary information. Any individuals who have a credit history indicating fiscal irresponsibility may not be assigned to finance or accounting positions.

For any individuals that will be working with minors or may have access to programs/events involving minors, a criminal background check is required. Any individuals who have criminal convictions that suggest that they could pose a threat to the health and safety of children may not be assigned to Trinity University if such assignment would involve access to or interaction with children. A social security number trace is also required so that the identity of the employee, independent contractor or agent can be verified.

For any individuals who will have access to residence halls or other secure areas a criminal background check is required. This group includes, but is not limited to residence hall assistants, supervisors and counselors; Physical Plant and janitorial staff; food services, concessions, and auxiliary services personnel. Any individuals who have a criminal history may not be assigned to Trinity University if such assignment would involve access to residence halls or secure areas. This check must also include a social security trace to ensure identity.

C. Breach

If the SERVICE PROVIDER experiences a security breach concerning any Confidential Information, then the SERVICE PROVIDER will:

a. fully comply with its obligations under any applicable law;

b. immediately notify the UNIVERSITY; and

c. fully cooperate with the UNIVERSITY in carrying out its obligations under any applicable law.

D. Return or Destruction of Confidential Information

Upon termination, cancellation, expiration or other conclusion of the Agreement, the SERVICE PROVIDER shall return to the UNIVERSITY or, if return is not feasible, destroy all Confidential Information in whatever form or medium that the SERVICE PROVIDER received from or created on behalf of the UNIVERSITY. This provision shall also apply to all Confidential Information that is in the possession of the SERVICE PROVIDER's contractors, consultants or agents, etc. In such case, the SERVICE PROVIDER shall retain no copies of such information, including any compilations derived from and allowing identification of Confidential Information. The SERVICE PROVIDER shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, the SERVICE PROVIDER shall certify in writing to the UNIVERSITY that such return or destruction has been completed.

If the SERVICE PROVIDER believes that the return or destruction of Confidential Information is not feasible, the SERVICE PROVIDER shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, the SERVICE PROVIDER shall extend the protections of this Agreement to Confidential Information received from or created on behalf of the UNIVERSITY, and limit further uses and disclosures of such Confidential Information for so long as the SERVICE PROVIDER maintains the Confidential Information.

E. Subcontractors, Vendors, and Agents

If SERVICE PROVIDER provides any Confidential Information which was received from, or created for UNIVERSITY to a subcontractor, vendor, agent or other project participants, then SERVICE PROVIDER shall require such subcontractor, vendor, agent, or other project participant to agree to the same restrictions and conditions as are imposed on SERVICE PROVIDER by this Agreement.

F. Maintenance of the Security of Electronic Information

SERVICE PROVIDER shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Confidential Information received from, or on behalf of UNIVERSITY.

G. Reporting of Unauthorized Disclosures or Misuses of Covered Data and Information

SERVICE PROVIDER shall report to UNIVERSITY any use or disclosure of Confidential Information not authorized by this Agreement or in writing by UNIVERSITY. SERVICE PROVIDER shall make the report to UNIVERSITY not more than one (1) business day after SERVICE PROVIDER learns of such use or disclosure.

H. Violation

Failure to abide by the requirements of legally applicable security measures and disclosure and re-disclosure restrictions may, in the UNIVERSITY'S sole discretion, result in the interruption, suspension and/or termination of the relationship with SERVICE PROVIDER. Violation of this Agreement constitutes unacceptable use of UNIVERSITY resources, and may violate other UNIVERSITY policies and/or state and federal law. Violations of the Agreement will result in severance of SERVICE PROVIDER contract with UNIVERSITY and may preclude SERVICE PROVIDER from future contracts with UNIVERSITY.

I. Survival

The SERVICE PROVIDER understands that the SERVICE PROVIDER'S obligations under this Agreement will continue after the SERVICE PROVIDER's relationship with the UNIVERSITY ends.

J. Privilege

The SERVICE PROVIDER's privileges hereunder are subject to periodic review, revision, and, if appropriate, renewal. The UNIVERSITY may at any time revoke the SERVICE PROVIDER'S access to Confidential Information. Access to Confidential Information is a privilege granted by the UNIVERSITY and is not a right.

K. Ownership Interest

The SERVICE PROVIDER has no right or ownership interest in any Confidential Information referred to in this Agreement.

L. Governing Law

This Agreement shall be subject to and governed by the laws of the State of Texas, excluding any conflicts-of-law rule or principle that may refer the construction or interpretation of this Agreement to the laws of another state. Each of the parties hereby consents to the jurisdiction of the state and federal courts in the State of Texas. Venue for its enforcement shall be in Bexar County, Texas.

M. Indemnity

SERVICE PROVIDER agrees to indemnify, defend, and hold harmless the UNIVERSITY, its trustees, officers, agents, employees, guests and contractors from any and all liabilities, claims, demands, expenses or costs, including attorneys' fees, arising out of any breach by the SERVICE PROVIDER of the SERVICE PROVIDER's obligations or representations and warranties under this Agreement, and the acts or omissions of the SERVICE PROVIDER or any of their suppliers, officers, agents, guests, affiliates, or contractors with respect to providing the Services contemplated herein. Such right to indemnity under this Agreement shall be in addition to, rather than to the exclusion of, the rights of the UNIVERSITY at law or in equity. This Section shall survive any termination of this Agreement.

In no event will the UNIVERSITY or any of its trustees, officers, agents, employees, guests and contractors be liable to the SERVICE PROVIDER or any other person or entity for payment of any consequential, incidental, punitive or other special damages arising from a failure to perform its obligations under this Agreement, including but not limited to lost profits.

N. Term

This Agreement shall take effect upon execution and continue until termination of SERVICE PROVIDER'S Service Contract with the UNIVERSITY.

O. Termination

In addition to the rights of the parties established by any underlying Agreement, if the UNIVERSITY reasonably determines in good faith that the SERVICE PROVIDER has materially breached any of the SERVICE PROVIDER's obligations under this Agreement, the UNIVERSITY, in its sole discretion, shall have the right to:

a. Exercise any of its rights to reports, access and inspection under this Agreement; and/or

b. Require the SERVICE PROVIDER to submit to a plan of monitoring and reporting, as the UNIVERSITY may determine necessary to maintain compliance with this Agreement; and/or

c. Provide the SERVICE PROVIDER with a fifteen (15) day period to cure the breach; and/or

d. Terminate the Agreement immediately if the SERVICE PROVIDER has breached a material term of this Agreement and cure is not possible.

Before exercising any of these options, the UNIVERSITY shall provide written notice to the SERVICE PROVIDER describing the violation and the action it intends to take.

VII. ACKNOWLEDGMENT

In the event of a conflict between the two Agreements, the UNIVERSITY's Confidentiality Agreement shall prevail. IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

SERVICE PROVIDER:

Signature:_____

Date:_____

Name: _____

Company:_____

TRINITY UNIVERSITY:

Signature:_____

Date:_____

Name: _____