I. General

The Contractor will ensure the agreed upon products and services will be provided to, or on behalf of, the University in a fully compliant manner to enable the Contractor and University to meet all relevant laws, regulations, and contractual requirements. All parties agree to handle data and other information with a standard of care at least as rigorous as that specified in the University's minimum standards within Information Privacy Policy, which are hereby incorporated by reference into this Agreement. The University is bound by the Family Educational Rights and Privacy Act (FERPA) regarding the release of student education records and, in the event of conflict with the University Policy, FERPA will govern.

II. University Information Privacy and Security

Notwithstanding any additional Contractor compliance responsibilities specified in this Agreement, or the University Information Privacy and Security Terms and Conditions included herein, each party shall comply with all applicable international, national, state, and local laws and regulations ("Applicable Laws") in performing its duties under this Agreement. Each party is responsible for its own compliance with Applicable Laws.

In the situation where additional compliance responsibilities are assigned to Contractor, Contractor acknowledges and agrees to use commercially reasonable practices to comply with the requirements specified in the Contract. Any such requirements are required to be acknowledged and agreed to by the Contractor and the University prior to execution of the Contract by the parties.

III. University and Contractor Compliance Responsibilities

A. Contractor shall implement, maintain and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of protected or private risk data as defined by the University. Contractor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

B. All facilities used to store, process, or transmit data classified as High or Moderate risk will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Without express prior written approval from the University, such data may not be stored, processed, received, or transmitted outside of data centers located within the United States.

C. Contractor warrants that all data classified as High or Moderate risk will be encrypted in transmission and at rest where required by law or contractual obligation (including via web interface) and may warrant use of the Advanced Encryption Standard (AES) encryption algorithm or other strong encryption protocol, as negotiated by the University.

D. Contractor will use industry standard and up-to-date security tools and technologies such as antivirus protections, antimalware and ransomware protections, and intrusion prevention and detection methods in providing services under this Agreement.

IV. Data Transfer Upon Termination or Expiration

Unless the University requests in writing that such data be destroyed upon termination, cancellation, expiration, or other conclusion of this Agreement, Contractor shall return the High or Moderate risk University data to the data that is in the possession of subcontractors or agents of Contractor. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonable standards for the type of data being destroyed, e.g., *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Revision 1. Contractor

shall certify in writing to the University that such destruction or return has been completed. Notwithstanding the expiration or termination of this Agreement for any reason, the obligation of confidentiality set forth in this document shall remain in force.

V. Breach

A. Definition. For purposes of this article, the term, "Security or Privacy Breach," has the meaning given to it under Chapter 501.171, F.S., applicable state or federal rule, regulation, or contractual obligation.

B. Notice will be given to the University of any actual or suspected unauthorized disclosure of, access to or other breach of the data within 48 hours. In the event of actual or suspected unauthorized disclosure of, access to, or other breach of the data, the Contractor will comply with all state and federal laws and regulations applicable to such breach and will cooperate with the University in fulfilling its legal obligations.

VI. Indemnification

A. Contractor agrees it will indemnify the University for its violation of the Terms and Conditions herein, including but not limited to the cost of providing appropriate notice to all required parties and credit monitoring, credit rehabilitation, or other credit support services to individuals with information impacted by the actual or suspected breach.

B. The University has secured cyber insurance. Liability to the University arising from any acts or omissions of any Officer, employee or agent of the University working within the scope of his or her employment, resulting in a breach of this Agreement shall not exceed $20 million taken together., IF such liability is in tort, this provision does not waive any limits on sovereign immunity afforded the University under of sec. 768.29, F.S. Insurance shall only be liable for actual damages incurred by the University, and shall not be liable for any indirect, consequential or punitive damages or attorney's fees, claim or cause of action, regardless of form (tort, contract, statutory, or otherwise) arising out of, relating to, or any way connected with this Agreement or any Services provided hereunder may be bought by either party any later that two (2) years after the accrual of such claim or cause of action.

C. Costs Arising from Breach. In the event of a security Breach by the Contractor or its Subcontractor related to products and services it is providing to the University in this Agreement, any Breach may be grounds for immediate termination of this Agreement by the University. Such a determination will be made in the sole discretion of the University.

D. This section and its indemnity will survive the termination of this agreement.

VII. Right to Information Privacy and Security Audit

Contractor agrees that the University shall have the option to request a technology audit, including obtaining the Contractor's current System and Organization Controls (SOC) 2 Type 2 report. If Contractor has not conducted a SOC 2 Type 2 audit, the University may, in its sole discretion, require Contractor to complete the university's third-party risk self-assessment on an annual basis. Records pertaining to the Contractor's services shall be made available to auditors and the University during normal working hours for this purpose.