1. Confidentiality/Privacy

1.1. Confidentiality

In addition to what may be defined in the Agreement related to Contractor’s proprietary information, “Confidential Information” is further defined as any and all information relating to this Agreement (a) that is disclosed under this Agreement in oral, written, graphic, machine recognizable, and/or sample form, being clearly designated, labeled, or marked as confidential or its equivalent at the time of disclosure, or (b) that Recipient knows or should know to be confidential. This includes University’s data or University’s customer’s data that Contractor may hold, process or otherwise have access to. The terms “Discloser” and “Recipient” refer respectively to the party disclosing or receiving a specific item of Confidential Information. The parties agree that following a disclosure of Confidential Information, Consumer Information or Customer Information (as defined in this addendum), Recipient shall (i) protect Discloser’s Confidential Information using the same degree of care it uses to protect its own confidential information of similar importance, but not less than reasonable care; (ii) restrict disclosure of Confidential Information to only (a) those employees, agents or contractors on a need to know basis for performance under this Agreement and who are bound by confidentiality terms substantially similar to those in this Agreement, (b) such parties to which production may be required pursuant to any valid legal process, and (c) regulatory agencies having authority over Recipient, (iii) use Confidential Information only for performance under this Agreement; and (iv) promptly notify Discloser upon discovery of Recipient’s unauthorized use or disclosure of the Confidential Information. Confidential Information does not include information, which is or becomes available without restriction to the recipient or any other person through no wrongful act. All materials containing Confidential Information are and remain the Discloser’s property, and upon written request the Recipient will promptly return them, and all copies of them, except a single archival copy. Notwithstanding the foregoing, information regarding each party, which is in the public domain, shall not be considered Confidential Information.

1.2. HIPAA/FERPA

To the extent that any of University’s information or records in Contractor’s control or possession from time to time constitutes “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act (“HIPAA”) and regulations issued there under, or that constitutes “protected education records” as that is defined in the Family Education Rights and Privacy Act (“FERPA”) Contractor shall maintain the confidentiality and security of that information as required of University under HIPAA and FERPA respectively. Should the Parties execute a separate Business Associate agreement, such agreement shall govern over this section 1.2.

2. Information Security

2.1. Information Security General - For all types of services or products offered under this Agreement, Contractor hereby represents, warrants, covenants and agrees that Contractor will:

2.1.1. Notify UNIVERSITY’S Chief Information Security Officer in the event of discovery of, or receipt from any source of, any security issue involving Contractor’s hardware, firmware, and/or software. Such notice to UNIVERSITY’S Chief Information Security Officer shall include severity of and the risks posed by such breach, isolation, activity or security issue, and recommended corrective actions and means of mitigating risk.

2.1.2. Reasonably cooperate with all UNIVERSITY security investigations activities and correct any identified security problems within a jointly agreed upon timeframe.

2.1.3. Should any of Contractor’s services for University involve online payments or Payment Card payments, Contractor hereby certifies that such services are compliant, with and will remain compliant with during the term of this agreement, the most recent version of the Payment Card Industry (PCI) standard.

2.1.3.1. For a Contractor approved for connecting to the University network, if applicable to the relationship. The University may provide an unprotected and unmanaged wired network connection to the Internet at each building location the Contractor provides services. No additional access, wired or wireless, will be granted to the University’s network for processing Cardholder Data or Sensitive Authentication Data upon the date of this Agreement or in the future. The Company must provide equipment and labor to secure and connect their equipment to the provided unprotected and unmanaged wired network connection/s and ensure a system for disaster recovery providing continuity of its business.
and security of all Cardholder Data and Sensitive Authentication Data should a major disruption or failure occur. Contractor must abide by all network security policies of the University and its network providers. Contractor agrees that it will not use:

2.1.3.1. a University provided network connection, or
2.1.3.1.2. other non-cellular wireless transmission method (e.g. Bluetooth) for transmission of any information that the University has defined as Sensitive Information unless such use has received prior written approval by University.

2.1.3.2. Any information stored (i.e. servers, backups) during the term of the Agreement must adhere to proper disposal methods per PCI standards upon termination of this Agreement.

2.2. **Hosting/Contractor Internal Policies/Procedures (only for agreements including Contractor/3rd Party hosting/processing/transmitting of UAB data/information)**

Should Contractor be hosting/processing/transmitting UAB data/information Contractor hereby represents, warrants, covenants and agrees that Contractor will:

2.2.1. Comply with industry accepted security standards and baseline controls, which contribute to the confidentiality, privacy, integrity, and availability of Confidential Information and services provided by Contractor.

2.2.2. Provide upon request a SSAE-16 SOC 2 type II report which includes an audit and summary of its documented security plan for systems containing University information, which plan shall describe the architecture of Contractor’s systems, information placement within the systems, and the security controls in place.

2.2.3. Upon termination of the Agreement, return all University-owned data/information (in a form acceptable to University), or at University’s request destroy, all University-owned information/data in Contractor’s possession. Contractor shall provide written certification of such return or destruction to University within fifteen (15) days of contract termination and validation from University of which method is to be used. Contractor’s responsibilities under this section shall be at no cost to University.

3. **Miscellaneous**

3.1. **Contractor’s Limitation of Liability**

Limitations on Contractor’s liability, regardless of conflicting language elsewhere in the Agreement, shall not apply to claims related to Contractor’s breach of Confidentiality, as defined in this Addendum or, if applicable, claims related to Contractor’s breach of the Information Security sections of this Addendum.

3.2. **Written Agreement Governs**

The Parties agree that this written, executed agreement shall govern over any ‘click’ or electronic agreement that may have to be accepted in order to download, install, maintain, or otherwise use the products covered under this Agreement.

3.3. **Audit Rights** - Valid only for agreements that already include audit language. Such audit language is hereby deleted and replaced as follows:

Contractor may request, no more than once annually, written certification from University that University is in compliance with this Agreement. Should Contractor have reasonable belief that University is not in compliance, Contractor may provide information detailing such non-compliance and request University’s approval for an on-site audit. If approved by University, audit shall be conducted at a time/place and in a manner agreeable to both Parties and be conducted by Contractor directly, not by a third party.

4. **Warranty**

4.1. **Illicit Code** - For any software or software development provided by Contractor the following provisions shall apply:

Illicit Code is defined as any harmful or hidden programs or data incorporated therein that destroys or impairs the Software and/or data, thereby inhibiting or preventing University from using the Licensed Software as warranted. Contractor uses commercially available software to detect existence of illicit code prior to distributing such Licensed Software; however, Contractor cannot guarantee that any Licensed Software is free of illicit codes and other defects. During the term of a Licensed Software warranty period, or during the term of any Software Support Services as the case may be, like with any other material Licensed Software defect, if it is determined that Illicit Code is present, then Contractor will use commercially reasonable efforts to correct the affected Software and if it cannot do so in a reasonable period of time, replace the affected Software. Contractor will also reasonably assist University in curtailting the spread of the illicit Code. Contractor represents and warrants that there are no methods for gaining access to the Licensed Software or other computer resources or data of University (such as a master access key, ID password, back door or trap door) other than as otherwise set forth, and Contractor will not embed any device in the Licensed Software or take any action to disrupt or terminate University’s operation of the Licensed Software.

4.2. **Section 508 Rehabilitation Act Compliance**

Contractor hereby represents, warrants, covenants and agrees that Contractor will ensure that any web pages offered by Contractor meet and comply with Section 508 of the Rehabilitation Act of 1973. UAB accepts the accessibility standards set
forth in the World Wide Web Consortium's (W3C) Web Accessibility Initiative (WAI) as a means to meet Section 508 requirements.

Signature Lines
IN WITNESS WHEREOF, the parties have executed this Addendum as of the date last executed, below.

CONTRACTOR

____________________________________
Signature

__________________________
Date

__________________________
UNIVERSITY

Signature

__________________________
Date