AUBURN UNIVERSITY
AT MONTGOMERY

Data Security, Accessibility, and Privacy Appendix

ARTICLE 1 – PURPOSE AND SCOPE OF APPLICATION

A. This Data Security, Accessibility, and Privacy Appendix (Appendix or DSAP) is designed to supplement the relationship between ___________________________ (Contractor) and Auburn University at Montgomery (AUM) in order to protect AUM's Non-public Information and AUM Information Resources (defined below). This Appendix describes the data security, accessibility and privacy obligations of Contractor and its agents and sub-contractors that connect to AUM Information Resources and/or gain access to Non-public Information (defined below).

B. Contractor agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Contractor also agrees to impose, by written contract, the terms and conditions contained in this Appendix on any third party retained by Contractor to provide services for or on behalf of AUM.

ARTICLE 2 – DEFINED TERMS

A. Breach. Breach means the unauthorized acquisition, access, use or disclosure of Non-public Information.

B. Protected Information. Protected Information shall be defined as information that identifies or is capable of identifying a specific individual, including but not limited to personally-identifiable information, medical information other than Protected Health Information as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA regulations (including, but not limited to 45 CFR § 160.103), Cardholder Data (as currently defined by the Payment Card Industry Data Security Standard and Payment Application Standard Glossary of Terms, Abbreviations, and Acronyms), student records, or individual financial information that is subject to laws restricting the use and disclosure of such information, including but not limited to the federal Gramm- Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); the federal Fair and Accurate Credit Transactions Act (15 USC § 1601 *et seq.*) and the Fair Credit Reporting Act (15 USC § 1681 *et seq.*).

C. Non-public Information. Contractor's provision of services may involve access to certain information that AUM wishes to be protected from further use or disclosure. Non-public Information shall include, but not be limited to: (i) Protected Information; (ii) information AUM discloses, in writing, orally, or visually, to Contractor, or to which Contractor obtains access to in connection with the negotiation and performance of the services, and which relates to AUM, its students or employees, its third-party vendors or licensors, or any other individuals or entities that have made confidential information available to AUM or to Contractor acting on AUM's behalf (collectively, "AUM Users"), marked or otherwise identified as proprietary and/or confidential, or that, given the nature of the information, ought reasonably to be treated as proprietary and/or confidential; (iii) trade secrets; and (iv) business information.

D. AUM Information Resources. AUM Information Resources shall be defined as those devices, networks and related infrastructure that AUM owns, operates or has obtained for use to conduct AUM business. Devices include but are not limited to, AUM-owned or managed storage, processing, communications devices and related infrastructure on which AUM data is accessed, processed, stored, or communicated, and may include personally owned devices. Data includes, but is not limited to, Non-public Information, other AUM-created or managed business and research data, metadata, and credentials created by or issued on behalf of AUM.

ARTICLE 3 – ACCESS TO AUM INFORMATION RESOURCES

A. In any circumstance when Contractor is provided access to AUM Information Resources, it is solely Contractor's responsibility to ensure that its access does not result in any access by unauthorized individuals to AUM Information Resources.

B. Contractor shall limit the examination of AUM information to the least invasive degree of inspection required to provide the goods and/or services.

ARTICLE 4 – COMPLIANCE WITH APPLICABLE LAWS, FAIR INFORMATION PRACTICE AND AUM POLICIES

A. Contractor agrees to comply with all applicable state, federal and international laws, as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Protected Information. Additionally Contractor will comply as applicable with the *Fair Information Practice Principles*, as defined by the U.S. Department of Commerce (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf). Such principles would typically require Contractor to have a privacy policy, and a prominently-posted privacy statement or notice in conformance with such principles.

B. Contractor shall make available to AUM all products, systems, and documents necessary to allow AUM to audit Contractor's compliance with the terms of this DSAP.

ARTICLE 5 – PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF NON-PUBLIC INFORMATION

Contractor agrees to hold AUM's Non-public Information, and any information derived from such information, in strictest confidence. Contractor will not access, use or disclose Non-public Information other than to carry out the purposes for which AUM disclosed the Non-public Information to Contractor, except as required by applicable law, or as otherwise authorized in writing by AUM. For avoidance of doubt, this provision prohibits Contractor from using for its own benefit Non-public Information or any information derived from such information. If required by a court of competent jurisdiction or an administrative body to disclose Non-public Information, Contractor will notify AUM in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give AUM an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Contractor's transmission, transportation or storage of Non-public Information outside the United States, or access of Non-public Information from outside the United States, is prohibited except on prior written authorization by AUM.

ARTICLE 6 – SAFEGUARD STANDARD

Contractor will implement, maintain and use appropriate security measures to preserve the confidentiality, integrity and availability of the Non-public Information. All Protected Information stored on portable devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2. Contractor will ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Contractor has responsibility for the Non-public Information under the terms of this Appendix. Prior to agreeing to the terms of this Appendix, and periodically thereafter (no more frequently than annually) at AUM's request, Contractor will provide assurance, in the form of a third-party audit report or other documentation acceptable to AUM, such as SOC2 Type II, demonstrating that appropriate information security safeguards and controls are in place.

ARTICLE 7 – RETURN OR DESTRUCTION OF NON-PUBLIC INFORMATION

Within 30 days of the termination, cancellation, expiration or other conclusion of this Appendix, Contractor will return the Non-public Information to AUM unless AUM requests in writing that such data be destroyed. This provision will also apply to all Non-public Information that is in the possession of subcontractors or agents of Contractor. Such destruction will be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Contractor will certify in writing to AUM that such return or destruction has been completed. If Contractor believes that return or destruction of the Non-public Information is technically impossible or impractical, Contractor must provide AUM with a written statement of the reason that return or destruction by Contractor is technically impossible or impractical. If AUM determines that return or destruction is technically impossible or impractical, Contractor will continue to protect the Non-public Information in accordance with the terms of this Appendix.

ARTICLE 8 – BREACHES OF NON-PUBLIC INFORMATION

A. **Reporting of Breach**: Contractor will report any confirmed or suspected Breach to the AUM Chief Information Security Officer (ootadmin@aum.edu) immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after Contractor reasonably believes a Breach has or may have occurred. Contractor's report will identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Non-public Information accessed, used or disclosed, (iii) the person(s) who accessed, used, disclosed and/or received Non-public Information (if known), (iv) what Contractor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action Contractor has taken or will take to prevent future unauthorized access, use or disclosure. Contractor will provide such other information, including a written report, as reasonably requested by AUM. In the event of a suspected Breach, Contractor will keep AUM informed regularly of the progress of its investigation until the uncertainty is resolved.

B. **Coordination of Breach Response Activities**: Contractor will fully cooperate with AUM's investigation of any Breach involving Contractor and/or the services, including but not limited to making witnesses and documents available immediately upon Contractor's reporting of the Breach. Contractor's full cooperation will include but not be limited to Contractor:

   i. Immediately preserving any potential forensic evidence relating to the Breach, and remedying the Breach as quickly as circumstances permit;
   ii. Promptly (within 2 business days) designating a contact person to whom AUM will direct inquiries, and who will communicate Contractor responses to AUM inquiries;
   iii. As rapidly as circumstances permit, applying appropriate resources to remedy the Breach condition, investigate, document, restore AUM service(s) as directed by AUM, and undertake appropriate response activities;
   iv. Providing status reports to AUM on Breach response activities, either on a daily basis or a frequency approved by AUM;
   v. Coordinating all media, law enforcement, or other Breach notifications with AUM in advance of such notification(s), unless expressly prohibited by law; and
   vi. Ensuring that knowledgeable Contractor staff is available on short notice, if needed, to participate in AUM-initiated meetings and/or conference calls regarding the Breach.

C. **Grounds for Termination.** Any Breach shall be grounds for AUM's immediate termination of any agreement between the parties in the sole and exclusive discretion of AUM.

D. **Assistance in Litigation or Administrative Proceedings.** Contractor shall make itself and any employees, subcontractors, or agents assisting Contractor available to AUM at no cost to AUM to testify as witnesses, or otherwise, in the event of a Breach or other unauthorized disclosure of Non-public Information caused by Contractor that results in litigation, governmental investigations, or administrative proceedings against AUM, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy or arising out of this Appendix.

ARTICLE 9 – DATA SECURITY AND PRIVACY STANDARD FOR PAYMENT CARD DATA (IF APPLICABLE)

A. Contractor agrees that it is responsible for the security of Cardholder Data (as currently defined by the Payment Card Industry Data Security Standard and Payment Application Standard Glossary of Terms, Abbreviations, and Acronyms) that it possesses (if any), including the functions relating to storing, processing and transmitting Cardholder Data.

B. Contractor affirms that, as of the effective date of this Addendum, it has complied with all applicable requirements of the PCI-DSS and has performed the necessary steps to validate its compliance with the PCI-DSS including undergoing a Level 2, or Level 1, PCI audit as necessary. Contractor agrees to provide upon execution of this agreement, and at least annually, and from time to time at the written request of AUM, current evidence (in form and substance reasonably satisfactory to AUM) of compliance with these data security standards, which has been properly certified by an authority recognized by the payment card industry for that purpose.

C. Contractor further represents and warrants that software applications it provides for the purpose of performing services related to processing credit card payments, are developed in accordance with all applicable standards, including but not limited to Payment Application Data Security Standards (PA-DSS), Point to Point Encryption Solution Requirements (P2PE) including approved card readers (PTS) or Point of Interaction (POI). Contractor agrees to provide, upon execution of this agreement, and at least annually, and from time to time upon written request of AUM, current evidence (in form and substance reasonably satisfactory to AUM) that any such application it provides is certified as complying with these standards and agrees to continue to maintain that certification as may be required.

D. In connection with credit card transactions processed for AUM, Contractor will provide reasonable care and efforts to detect fraudulent payment card activity. In performing the services, Contractor will comply with all applicable rules and requirements, including security rules and requirements, of AUM's financial institutions, including its acquiring bank, the major payment card associations and payment card companies. If during the term of an Agreement with AUM, Contractor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI standards and/or other material payment card industry standards, it will promptly notify AUM of such circumstances.

E. Contractor will immediately notify AUM if it learns that it, or any of its PCI-DSS service providers, is no longer PCI compliant under one of the standards identified above, or if any software applications or encryption solutions are no longer PA-DSS, PTS-DSS or P2PE compliant. Should Contractor, or its service provider, fail to recertify as compliant to the appropriate PCI standard within a timeframe deemed reasonable by AUM, AUM shall, at its discretion terminate this agreement.

F. Contractor shall be responsible for implementing and monitoring all PCI-DSS requirements for devices, networks and processes located on the Contractor's premises, private networks extended onto AUM premises, as well as maintenance of devices and applications for which the Contractor maintains administrative control. Contractor shall complete necessary PCI-DSS vulnerability and penetration tests on devices on its networks or private networks extended onto the AUM campus. AUM shall be responsible for all PCI-DSS requirements for devices, networks and processes located on AUM premises, and for devices for which it maintains sole administrative control. AUM shall complete necessary vulnerability scans and penetration tests on devices on networks under its control. AUM shall be responsible for physical security of Contractor devices located on AUM's premises.

ARTICLE 10 – ACCESSIBILITY STANDARDS

AUM affords equal opportunity to individuals in its employment, services, programs, and activities in accordance with the Americans with Disabilities Act and Section 504 of the 1973 Rehabilitation Act. This includes effective communication and access to electronic and information technology resources for individuals with disabilities. To comply with AU's accessibility standards, Contractor represents and warrants that it shall:

A. Read, review, and understand Auburn University's Electronic and Information Technology Accessibility Policy and associated definitions (https://sites.auburn.edu/admin/universitypolicies/Policies/ElectronicandInformationTechnologyAccessibilityPolicy.pdf);
B. Develop software and web applications that complies with the Policy and Standards which currently require compliance with WCAG 2.0 Level A and AA;
C. Prior to delivery of any software or web applications, test it for compliance with the applicable Standards and report testing results to university in a format specified by AUM;
D. Use best commercial efforts to modify the software to maximize accessibility compliance and otherwise resolve any identified accessibility compliance issues;
E. Deliver software that complies with AU's Policy and Standards, to the extent feasible as determined by university. Pending verification of compliance with this provision, AUM is authorized, but not required, to withhold any payment to Software and Web Developer pursuant to this agreement. If vendor is unable to comply with AU Policy and Standards then AUM shall have the option to terminate all agreements with vendor without any liability. Software shall not be considered in compliance with this provision unless or until the University Chief Information Officer or designee has approved

ARTICLE 11 – ATTORNEY'S FEES

In any action brought by a party to enforce the terms of this Appendix, the prevailing party will be entitled to reasonable attorney's fees and costs, including the reasonable value of any services provided by in-house counsel. The reasonable value of services provided by in-house counsel will be calculated by applying an hourly rate commensurate with prevailing market rates charged by attorneys in private practice for such services.

ARTICLE 12 – INDEMNITY

Contractor shall indemnify, hold harmless and defend AUM, its Board of Trustees, Trustees individually, Administrators, Faculty, Staff, and Agents, from and against any and all loss, damage or liability resulting from demands, claims, suits, or actions of any character presented or brought for any injuries, including death, to persons or for damages to property caused by or arising out of any negligent (including strict liability), wanton, reckless, or intentional act or omission of Contractor, any of its subcontractors, invitees, guests, employees, or agents, or which otherwise arises out of, relates to, or is attributable to, User's duties under this DSAP. This indemnity shall apply whether the same is caused by or arises out of the joint, concurrent, or contributory negligence of any person or entity. The foregoing indemnity shall include, but not be limited to, court costs, attorney's fees, costs of investigation, costs of defense, settlements, and judgments associated with such demands, claims, suits or actions For the avoidance of doubt regarding a Breach involving Protected Information, Contractor's indemnification obligations under the Appendix will include, but not be limited to, the following fees and costs which arise as a result of Contractor's breach of this Appendix, negligent acts or omissions, or willful misconduct: any and all costs associated with notification to individuals or remedial measures offered to individuals, whether or not required by law, including but not limited to costs of notification of individuals, establishment and operation of call center(s), credit monitoring and/or identity restoration services; time of AUM personnel responding to Breach; fees and costs incurred in litigation; the cost of external investigations; civil or criminal penalties levied against AUM; civil judgments entered against AUM; attorney's fees, and court costs.

ARTICLE 13 – ADDITIONAL INSURANCE

In addition to the insurance required under the Agreement, Contractor at its sole cost and expense will obtain, keep in force, and maintain an insurance policy (or policies) that provides coverage for privacy and data security breaches. This specific type of insurance is typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability. In some cases, Professional Liability policies may include some coverage for privacy and/or data breaches. Regardless of the type of policy in place, it needs to include coverage for reasonable costs in investigating and responding to privacy and/or data breaches with the following minimum limits unless AUM specifies otherwise: $1,000,000 Each Occurrence and $5,000,000Aggregate.

ARTICLE 14 – SURVIVAL: ORDER OF PRECEDENCE

This DSAP shall survive the expiration or earlier termination of any agreement between AUM and Contractor. In the event the provisions of this DSAP conflict with any provision of the of any agreement between Contractor and AUM, or Contractors' warranties, support contract, or service level agreement, the provisions of this DSAP shall prevail.

Contractor Acceptance

Signed: ________________________________ Date: ______________________________________

Name: __________________________________ Phone: _____________________________________

Title: __________________________________ Email: ______________________________________