Requirements for the Protection of Carthage College's
Protected Information

Effective as of _____, this Rider is added to and incorporated as part of the [agreement name] (in this Rider, the "Agreement"), dated as of _____, between Carthage College (in this Rider, "College") and _____ (in this Rider, "Vendor"). Capitalized terms not defined in this Rider shall have the meaning provided in the Agreement. In the event of any conflict between the terms of this Rider and the Agreement, the terms of this Rider shall govern.

A. Acknowledgement of Confidential Nature of Information, Access and Applicable Law

Vendor acknowledges that its performance of Services under this Agreement may involve access to Confidential Information of the College including, but not limited to, personally-identifiable information, student records, protected health information, or individual financial information (collectively, "Protected Information") that is subject to state, federal and/or international laws/rules 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)); and the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Health Insurance Portability and Accountability Act and its implementing regulations (including without limitation 45 CFR Part 160 and Subparts A, C, and E of Part 164); and Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation), as well as any national, state or territorial implementations of such laws (as may be amended, superseded or replaced) (collectively, "GDPR"). Vendor agrees to comply, and require subcontractors to comply, with all applicable federal, state and international laws restricting the access, use and disclosure of Protected Information.

B. Prohibition on Unauthorized Use or Disclosure of Protected Information

Vendor agrees to hold the College's Protected Information, and any information derived from such information, in strictest confidence. Vendor shall not access, use or disclose Protected Information except as permitted or required by the agreement or as otherwise authorized in writing by the College, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected Information, Vendor will notify College in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give College an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). If such opposition is unsuccessful, or if the College does not otherwise oppose or respond to the disclosure notice, Vendor shall provide to the College a copy of any Protected Information disclosed contemporaneously with its disclosure. Any transmission, transportation or storage of Protected Information outside the United States is prohibited except on prior written authorization by the College. Notwithstanding any other provisions of this Agreement, this Section B does not prohibit or limit Vendor from any use or disclosure of any information that may be the same as any Protected Information but which Vendor can demonstrate by documentary evidence was (i) properly obtained by Vendor without access to, reference to or use of any Protected Information, and (ii) at all times maintained separately from and not in any way combined, commingled, compared, benchmarked or in any way associated with any Protected Information.

C. Safeguard Standard

With respect to the College's Protected Information, Vendor shall comply in all respects reasonably pertinent to the Agreement with the Fair Information Practice Principles, as defined by the U.S. Federal Trade Commission. If collecting Protected Information electronically from individuals on behalf of the College, Vendor shall utilize a privacy statement or notice in conformance with such principles. Vendor agrees to protect the privacy and security of Protected Information according to all applicable laws and regulations, by industry standard & commercially-acceptable standards, and no less rigorously than it protects its own confidential information. Vendor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality (authorized access), integrity and availability of the Protected Information. While Vendor has responsibility for the Protected Information under the terms of this Agreement, Vendor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities. 1. All facilities used to store and process Protected Information will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. 2. Without limiting the foregoing, Vendor warrants that all Protected Information will be encrypted in transmission (including via web interface) and encrypted in storage at no less than 128bit level encryption. 3. Vendor will use industry standard and up-to-date security tools and technologies such as antivirus protections, multi-factor authentication, and intrusion detection methods in providing Services under this Agreement. 4. Vendor shall not store or process Protected Information outside of data centers located in the United States without prior approval from College.

D. GDPR Compliance

For purposes of this section, Controller, Processor, Data Subject, processing and appropriate technical and organizational measures have the meanings as defined in GDPR. The parties acknowledge that for GDPR purposes, the College is the Controller and Vendor is the Processor, and that Vendor shall process Protected Information (i) for the purposes described in the Agreement; and/or (ii) as may otherwise be permitted under GDPR. The College must consent in writing and in advance to the Provider appointing a third-party processor of Protected Information under this agreement. Such consent will only be given if Vendor confirms that it has entered with the third-party processor into a written agreement incorporating terms which are substantially similar to those set out in this Agreement (including this Rider) and in any case which the College confirms will reflect the requirements of GDPR. As between the College and Vendor, Vendor shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this Rider. To the extent the College transfers Protected Information to Vendor and Vendor is located in a territory outside the European Economic Area ("EEA") that does not provide adequate protection for Protected Information (as determined by GDPR), Vendor agrees to abide by and process such Protected Information in accordance with the Standard Contractual Clauses for Controllers as approved by the European Commission and available at http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32004D0915 (as amended, superseded or replaced from time to time) ("Model Clauses"), which are incorporated by reference in, and form an integral part of, this Rider. Vendor agrees that it is a "data importer" and the College is the "data

exporter" under the Model Clauses (notwithstanding that the College is an entity located outside of the EEA).

E. Return or Destruction of Protected Information

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, Vendor shall return the Protected Information to College in an agreed upon format, unless the College requests in writing that such data be destroyed. This provision shall also apply to all Protected Information that is in the possession of subcontractors or agents of Vendor. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonably standards for the type of data being destroyed (e.g. Guidelines for Media Sanitization, NIST SP 800-88). Vendor shall certify in writing to College that such return or destruction has been completed.

F. Breaches of Protected Information

For purposes of this section, the term "Breach," has the meaning given to it under the applicable state, federal or international law and/or regulation.

1. Reporting of Breach. Immediately upon discovery of a confirmed or suspected Breach, Vendor shall report both orally and in writing to the College. In no event shall the report be made more than two (2) business days after Vendor knows or reasonably suspects a Breach has or may have occurred. Notifications must be made to the College prior to any public disclosures. In the event of a suspected Breach, Vendor shall keep the College informed regularly of the progress of its investigation until the uncertainty is resolved.

   Vendor's report shall identify:

   1. The nature of the unauthorized access, use or disclosure,
   2. The Protected Information accessed, used or disclosed,
   3. The person(s) who accessed, used and disclosed and/or received Protected or Private Information (if known),
   4. What Vendor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
   5. What corrective action Vendor has taken or will take to prevent future unauthorized access, use or disclosure.
   6. Vendor shall provide such other information, including a written report, as reasonably requested by College.

2. Coordination of Breach Response Activities.

In the event of a Breach, Vendor will:

   1. Immediately preserve any potential forensic evidence relating to the Breach;
   2. Promptly (within 2 business days) designate a contact person to whom the College will direct inquiries, and who will communicate Vendor responses to College inquiries;
   3. As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore College service(s) as directed by the College, and undertake appropriate response activities;

4. Provide status reports to the College on Breach response activities, either on a daily basis or a frequency approved by the College;
5. Coordinate all media, law enforcement, or other Breach notifications with the College in advance of such notification(s), unless expressly prohibited by law;
6. Make all reasonable efforts to assist and cooperate with the College in its Breach response efforts;
7. Ensure that knowledgeable Vendor staff are available on short notice, if needed, to participate in College-initiated meetings and/or conference calls regarding the Breach.

3. Costs Arising from Breach.

In the event of a Breach by the Vendor or its staff or subcontractors, Vendor agrees to promptly reimburse all costs to the College arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of College personnel responding to Breach, civil or criminal penalties levied against the College, attorney's fees, court costs, etc. Any Breach may be grounds for termination of this Agreement by the College.

G. End User Agreements

Any agreements or understandings, whether electronic, click through, verbal or in writing, between Vendor and College employees or other end users under this Agreement that conflict with the terms of this Agreement, shall not be valid or binding on the College or any such end users. Revisions are acceptable provided that such revision does not materially affect, reduce or diminish the services provided to College under this Agreement or otherwise impose additional or more restrictive obligations upon College than those imposed in this Agreement.

H. Examination of Records

College shall have access to and the right to examine any pertinent books, documents, papers, and records of Vendor involving transactions and work related to this agreement until the expiration of five years after final payment hereunder. Upon request, Vendor shall provide the most current SOC2 and HECVAT reports for its service, as well as SOC2 reports for its underlying hosting services.

I. Assistance in Litigation or Administrative Proceedings

Vendor shall make itself and any employees, subcontractors, or agents assisting Vendor in the performance of its obligations under the Agreement available to College at no cost to College to testify as witnesses in the event of an unauthorized disclosure caused by Vendor that results in litigation or administrative proceedings against College, its directors, officers, agents or employees based upon a claimed violation of laws relating to security, privacy or arising out of this agreement.

J. Insurance

Vendor shall maintain at all times during the term of this Agreement, at its own expense, cyber liability insurance with limits of no less than $1,000,000.00 for any one occurrence and $4,000,000.00 in annual aggregate.

K. Survival

The Vendor shall maintain an industry standard disaster recovery program to reduce in potential effect of outages because of supporting data center outages. Any backup site used to store College Protected Information shall include the same information security and privacy controls as the primary data center(s). Vendor shall apply industry standards to protect against ransomware (including air gaps and immutable backups)

L. Right to Audit

Vendor agrees that, as required by applicable state and federal law, auditors from state, federal, the College, or other agencies so designated by the College, shall have the option to audit the outsourced service. Records pertaining to the service shall be made available to auditors and the College during normal working hours for this purpose.

For Vendor	For College
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____