

## TEMPLATE LANGUAGE RE: CONFIDENTIALITY AND SECURITY

### 1.0 CONFIDENTIALITY AND SECURITY:

- 1.1 The term “Confidential Information” shall mean this Agreement and all proprietary information, data, trade secrets, business information, any personally identifiable information regarding students, employees or other individuals or entities, including but not limited to, Social Security numbers, other tax identification numbers, credit card, bank account and other financial information, and other information of any kind whatsoever which: (a) a Party (“Discloser”) discloses, in writing, orally or visually, to the other Party (“Recipient”) or to which Recipient obtains access in connection with the negotiation and performance of this Agreement, and which (b) relates to: (i) the Discloser, or (ii) in the case of Service Provider as Recipient, University, its students and employees, and its third-party vendors or licensors who have made confidential or proprietary information available to University. University Confidential Information shall include Personally Identifiable Information, as described below. Service Provider acknowledges that University has a responsibility to its students and employees to keep information about its students and employees and their records and accounts (“Personally Identifiable Information”) strictly confidential. Service Provider represents and warrants that it will keep such Personally Identifiable Information strictly confidential both during the Term and after the termination of the Agreement.
- 1.2. Service Provider shall not disclose or use University Confidential Information other than to carry out the purposes for which University or one of its Affiliates disclosed such University Confidential Information to Service Provider. Service Provider shall not disclose any University Confidential Information other than on a “need to know” basis and then only to: (a) its employees or officers, provided, however that each such employee or officer have entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof; (b) Affiliates of Service Provider, only if approved by University and provided that such Affiliates shall be restricted in use and redisclosure of University Confidential Information to the same extent as Service Provider, and provided further that the Affiliate’s employees or officers have each entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof; (c) to Subcontractors, only if approved by University and provided further that such Subcontractors and each of their employees and officers have entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof; (d) to independent contractors, agents, and consultants hired or engaged by University, provided, however, that University has instructed Service Provider to provide such information or if Service Provider has confirmed that all such persons are subject to a confidentiality agreement, enforceable under the laws of the United States, California and each applicable non-U.S. jurisdiction, which shall be no less restrictive than the provisions of this Section; or (e) as required by applicable law and regulation, order of any court or government agency or rule of a self-regulatory agency (collectively, “Legal Process”), or as otherwise permitted by this Agreement, either during the Term of this Agreement or

after the termination of this Agreement. The restrictions set forth herein shall apply during the Term and after the termination of this Agreement.

- 1.3 Prior to any disclosure of Confidential Information as required by Legal Process, the Recipient shall: (i) notify the Discloser of any, actual or threatened legal compulsion of disclosure, and any actual legal obligation of disclosure immediately upon becoming so obligated, and (ii) reasonably cooperate with the Discloser's reasonable, lawful efforts to resist, limit or delay disclosure.
- 1.4. All Work Product, works-in-progress, notes, data, reference materials, memoranda, documentation and records in any way incorporating or reflecting any of University Confidential Information and all proprietary rights therein, including copyrights, will belong exclusively to University. Upon the termination or expiration of this Agreement, or at any time upon the request of University, Service Provider shall return all University Confidential Information (and all copies and derivative works thereof made by or for Service Provider), including Personally Identifiable Information, in the possession of Service Provider or in the possession of any third party over which Service Provider has or may exercise control and further shall delete or erase such Confidential Information, copies and derivative works thereof, from computer systems in the possession or control of Service Provider or any third party acquiring University's Confidential Information from Service Provider. University shall have the right to require Service Provider to verify, to University's satisfaction, that all University Confidential Information has been returned. Service Provider agrees to fully cooperate with University's requests for verification. Verification may include University conducting an on-site audit of Service Provider's systems and facilities and/or Service Provider executing a sworn affidavit stating that it does not have in its possession or under its control any other documents, contracts, computer code, computer data or other materials, in tangible or electronic form, that pertain to University Confidential Information.
- 1.5. **Exceptions to Obligations of Confidentiality.** With the exception of the obligations related to Personally Identifiable Information, the obligations of confidentiality in this Section shall not apply to any information that (a) Recipient rightfully has in its possession when disclosed to it, free of obligation to Discloser to maintain its confidentiality; (b) Recipient independently develops without access to Discloser's Confidential Information; (c) is or becomes known to the public other than by breach of this Section; (d) Discloser or its agent releases without restriction; or (e) Recipient rightfully receives from a third party without the obligation of confidentiality. Any combination of Confidential Information disclosed with information not so classified shall not be deemed to be within one of the foregoing exclusions merely because individual portions of such combination are free of any confidentiality obligation or are separately known in the public domain.
- 1.6. Service Provider agrees that under no circumstances shall any of Service Provider's employees, officers, Affiliates or Subcontractors, whether full-time or part-time, connect to any University system or handle any University data, for purposes of downloading, extracting, storing or transmitting information through personally owned,

rented or borrowed equipment including, but not limited to, laptops, Blackberries/palm pilots and cell phones. Any exceptions are at variance with University policy and must be approved in advance according to University policy guidelines.

- 1.7. **No License Conferred.** All Confidential Information shall remain the property of the Discloser or its licensors. Except to the extent expressly provided herein, this Agreement shall not be construed as conferring on a Recipient an express or implied license or an option for a license for any patent, copyright, trademark, license right or trade secret owned or obtained by the Discloser.
- 1.8 **Media Releases.** All media releases, public announcements and public disclosures by either Party, or their Representatives, employees or agents, relating to this Agreement or the name or logo of University, any University Affiliate, any other business entity under common control with University, or Service Provider, including, without limitation, promotional or marketing material, but not including any disclosure required by legal, accounting or regulatory requirements beyond the reasonable control of the releasing Party, shall be coordinated with and approved by the other Party in writing prior to the release thereof.
- 1.9 **Information Security Plan.** Service Provider acknowledges that University is required to comply with information security standards for the protection of Personally Identifiable Information and other Confidential Information required by law, regulation and regulatory guidance, as well as University's internal security program for information and systems protection.

Within thirty (30) days of the Effective Date of the Agreement and subject to the review and approval of University, Service Provider shall establish, maintain and comply with an information security plan ("Information Security Plan"), which shall contain such elements that University may require after consultation with Service Provider.

On at least an annual basis, Service Provider shall review, update and revise its Information Security Plan, subject to University's review and approval. At University's request, Service Provider shall make modifications to its Information Security Plan or to the procedures and practices thereunder to conform to University's security requirements as they exist from time to time.

Service Provider's Information Security Plan shall be designed to:

- Ensure the security, integrity and confidentiality of Confidential Information;
- Protect against any anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the person that is the subject of such information; and
- Comply with all applicable legal and regulatory requirements for data protection.

The parties expressly agree that Service Provider's security procedures shall require that any Personally Identifiable Information transmitted or stored by Service Provider only be transmitted or stored in an encrypted form approved by University.

- 1.10 **Notice of Security Breach.** Service Provider shall notify University's Relationship Manager and its designated principal security officer of any known or suspected security breach of its system or facilities containing University Confidential Information or any other breach of Confidential Information relating to this Agreement immediately, but not later than within twenty-four (24) hours after discovery, if the information was, or is reasonably believed to have been, acquired by an unauthorized person. Service Provider agrees to fully cooperate with University with the preparation and transmittal of any notice, which University may deem appropriate or required by law, to be sent to customers or other affected third parties regarding the known or suspected security breach, and to further take appropriate remedial action with respect to the integrity of its security systems and processes. Service Provider's Information Security Plan shall include a written response program addressing the appropriate remedial measures it shall undertake in the event that there is an information security breach.
- 1.11 Service Provider shall cause all Subcontractors and other persons and entities whose services are part of the Services which Service Provider delivers to University or who hold University Confidential Information and Personally Identifiable Information, to implement an information security program and plan substantially equivalent to Service Provider's.

In addition, Service Provider represents and warrants that in performing the Services, it will comply with all applicable privacy and data protection laws and regulations of the United States including, as applicable, the provisions in the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq., the Family Education Rights and Privacy Act ("FERPA"), 20 USC Section 1232(g) et seq., and of any other applicable non-U.S. jurisdiction, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission and other applicable guidance, to protect University's Personally Identifiable Information from identity theft, fraud and unauthorized use.

- 1.12 Service Provider represents and warrants that it shall implement and maintain certification of Payment Card Industry ("PCI") compliance standards regarding data security and that it shall undergo independent third party quarterly system scans that audit for all known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (*i.e.*, viruses and worms) to gain access to or disrupt the network devices. Service Provider agrees promptly to provide, from time to time at the request of the University, current evidence, in form and substance reasonably satisfactory to University, of compliance with these data security standards which has been properly certified by an authority recognized by the payment card industry for that purpose. Further, without limiting the provisions of

Section 5.1, Service Provider shall maintain and protect in accordance with all applicable federal, state, local, and PCI laws, rules and regulations the security of all cardholder data when performing the contracted Services on behalf of the University. Service Provider shall indemnify, defend, protect and hold University harmless from and against any and all claims, losses, damages, notices and expenses, including, without limitation, any fines which University maybe required to pay, which result from Service Provider's breach of the provisions of this Section 1.12. Without limiting the generality of the foregoing, it is expressly agreed that if University pays any fine in connection with a breach by Service Provider of the provisions of this Section 1.12, the foregoing indemnity obligation shall require Service Provider to reimburse University the full amount of such fine within thirty (30) days of University delivering written notice to Service Provider of University's payment of such fine. Service Provider, at its sole cost and expense, shall fully cooperate with any investigation, whether instituted by University or any other entity with jurisdiction to conduct such investigation, of any data loss or other breach of Service Provider's obligations under this Section 1.1.2. Service Provider shall not be held responsible for any such loss of data if it is shown that the loss occurred as a result of the sole negligence of the University. In connection with credit card transactions processed for University, Service Provider will provide reasonable care and efforts to detect fraudulent credit card activity. In performing the Services, Service Provider shall comply with all applicable rules and requirements, including security rules and requirements, of University's financial institutions, including its acquiring bank, the major credit card associations and credit card companies. If during the term of the Agreement, Service Provider 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 the University of such circumstances.

1.13 Service Provider represents and warrants that software applications it provides for the purpose of performing Services related to processing payments, particularly credit card payments, are developed in accordance with and are in compliance with the standards known as Payment Application Data Security Standards (PA-DSS) or Payment Applications Best Practices (PABP). As verification of this, the Service Provider agrees to provide evidence 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 from time to time.

1.14 Failure by Service Provider to comply with any provision of this Section shall constitute a material breach of the Agreement.

## **2.0 SUPPLIER PERSONNEL:**

2.1 Service Provider's personnel are not eligible to participate in any of the employee benefit or similar programs of University. Service Provider shall inform all of its personnel providing Services pursuant to this Agreement that they will not be considered employees of University for any purpose, and that University shall not be liable to any of them as an employer for any claims or causes of action arising out of or relating to their assignment.

- 2.2 Upon the written request of University for cause pursuant to this Agreement, Service Provider agrees to promptly review the conduct of and remove, as necessary, any of Service Provider's Representatives or Subcontractors performing Services under this Agreement and replace such Representative or Subcontractor as soon as practicable.
- 2.3 As a general matter, Service Provider shall not engage its Affiliates or Subcontractors for the performance of the Services. The engagement of an Affiliate or Subcontractor by Service Provider shall be subject to University's prior written consent and sole discretion, and shall not relieve Service Provider of any of its obligations under this Agreement. Service Provider shall require all Affiliates and Subcontractors, as a condition to their engagement, to agree to be bound by provisions substantially the same as those included in this Agreement, and in particular, the Sections regarding Service Provider personnel, insurance, and confidentiality and security. Upon University's request, Service Provider shall provide documentation evidencing its Affiliates' and Subcontractors' compliance with these provisions. Service Provider shall further provide University with a listing, which it shall update from time to time, identifying each location or facility of it, its Affiliates, and its Subcontractors, at which Services are performed or University Confidential Information is stored. Any work to be performed in connection with this Agreement by Service Provider, its Affiliates or Subcontractors must be performed in the United States, unless the prior written consent of the University is received to perform work outside the United States. Further, University Confidential Information may not be transmitted or stored outside the United States without the prior written consent of University.
- 2.4 Service Provider shall comply and shall cause its Representatives, Affiliates and Subcontractors to comply with all personnel, facility, safety and security rules and regulations and other instructions of University, when performing work at a University facility, and shall conduct its work at University facilities in such a manner as to avoid endangering the safety, or interfering with the convenience of, University Representatives or customers. Service Provider agrees that it, its Representatives and Subcontractors providing Services hereunder, shall possess any licenses, approvals or certifications required by any applicable law or regulatory agency or self-regulatory organization.
- 2.5 Service Provider shall not knowingly permit a Representative or Subcontractor to have access to the records, data or premises of University when such Representative or Subcontractor: (a) has been (i) convicted of a crime or has engaged in (ii) a dishonest act or a breach of trust; or (b) uses illegal drugs.
- 2.6 Service Provider represents that it maintains comprehensive hiring policies and procedures which include, among other things, a background check for criminal convictions, and pre-employment drug testing, all to the extent permitted by law. Service Provider shall conduct thorough background checks and obtain references for all its Representatives and Subcontractors performing the Services. Service Provider further represents that through its hiring policies and procedures, it uses commercially practicable efforts to hire candidates with appropriate character,

disposition, and honesty. Service Provider shall require all Subcontractors, as a condition to their engagement, to be bound by the provisions of this Section. To satisfy Service Provider's obligations under this Section, University may require Service Provider to utilize the services of a third party service provider designated by University to obtain the required background investigations.

- 2.7 University shall notify Service Provider of any act of dishonesty committed against University which may involve a Service Provider Representative or Subcontractor, and Service Provider shall promptly notify University if it becomes aware of any such offense. Following such notice, at the request of University and to the extent permitted by law, Service Provider shall cooperate with investigations conducted by or on behalf of University. Service Provider agrees to pursue all available legal action against any employee who has committed a crime, fraud or tort during the course of performing Services for University.
- 2.8 Service Provider shall provide University with an escalation list of names and contact information for middle and senior management responsible in each jurisdiction for the oversight and monitoring of the employees performing the Services. Service Provider further represents and warrants that it will commit sufficient management resources and staff to meet the performance requirements for the Services set forth in this Agreement.

### **3.0 FINANCIAL RESPONSIBILITY AND AUDIT:**

- 3.1 **Retention of Records.** Service Provider shall maintain at no additional cost to University, in a reasonably accessible location identified to University, all records pertaining to the Services provided to University under this Agreement for a period of two (2) years or longer after termination of the Agreement, if required by applicable law or regulation. Service Provider further agrees to provide to University, at its request, a full copy of all such records for University to maintain at a U.S. location which University shall designate.
- 3.2 **Annual Financial and Operational Audits.** Within thirty (30) days of the Effective Date of the Agreement, Service Provider shall provide University with copies of its latest financial audit and its operational audits for the facilities being used to provide Services under this Agreement. Thereafter, Service Provider shall conduct such audits at least annually, at its sole cost and expense. Service Provider shall provide University with a copy of each report prepared in connection with each such audit within thirty (30) calendar days after it prepares or receives such report. The audits must be performed as full SAS 70 audits and if specified by University, Service Provider must be able to meet other key international security and audit certifications (e.g., ISO 17799 or BS 7799). Notwithstanding the foregoing, Service Provider shall notify University immediately in the event there is a change of control or material adverse change in its business or financial condition that may affect Service Provider's ability to perform the Services.
- 3.3 During regular business hours, University may, at its sole expense and on a mutually

agreed upon date (which shall be no more than fourteen (14) days after written notice), time, location and duration perform or arrange for a site visit and/or confidential audit of Service Provider's operations, facilities, financial records, and security and business continuity systems which pertain specifically to the Services. If Service Provider is not in substantial compliance with the requirements of the performance requirements set forth in this Agreement, University shall be entitled, at Service Provider's expense, to perform additional such audits. University will provide to Service Provider a copy of each report prepared in connection with any such audit within thirty (30) calendar days after it prepares or receives such report. Service Provider agrees to promptly take action at its expense to correct those matters or items that require correction as mutually agreed. If any audit discloses material variances from the performance requirements set forth in this Agreement or a material breach by Service Provider of the provisions of this Agreement, Service Provider shall be deemed in default of this Agreement.

3.4 Service Provider will give prior notice to University of requests by regulatory authorities to examine Service Provider's records regarding University. At University's written request, Service Provider shall reasonably cooperate with University in seeking a protective order with respect to such records. Service Provider agrees to submit to and cooperate with any requests for information or examination by regulatory entities with supervisory authority over University.

4.0 **NON-ASSIGNMENT:** Neither Party may assign this Agreement or any of the rights hereunder or delegate any of its obligations hereunder, without the prior written consent of the other Party, and any such attempted assignment shall be void.

#### 5.0 **COMPLIANCE WITH LAWS:**

5.1 Service Provider shall comply with all applicable United States federal, state and local laws, regulations and ordinances, and rules of self-regulatory organizations, including National Automated Clearing House Association ("NACHA") rules, as well as all national, state and local laws, regulations and ordinances, and rules of self-regulatory organizations of any other non-U.S. jurisdiction to which Service Provider, University or the Services are subject. If a charge of non-compliance with such laws, regulations and rules is brought against Service Provider in connection with this Agreement or the Services, Service Provider shall promptly notify University of the charge in writing. Service Provider shall indemnify and hold University harmless from any damages or costs incurred as a result of any finding or ruling by a court or government body or self-regulatory organization that Service Provider's provision of the Services hereunder violates any laws or regulations promulgated under the United States or other jurisdiction.

#### 6.0 **DEFINITIONS**

6.1 Affiliate - an entity now or hereafter controlled by, controlling or under common control with a Party. Control exists when an entity owns or controls more than 50% of

the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity.

- 6.2 Party - University or Service Provider.
- 6.3 Representative - an employee, officer, director, or agent of a Party.
- 6.4 Relationship Manager - the respective employees of each Party that each Party shall designate to act on its behalf with regard to matters arising under this Agreement; each Party shall notify the other in writing of the name of their Relationship Manager; however, the Relationship Manager shall have no authority to alter or amend any term, condition or provision of the Agreement; further, each Party may change its Relationship Manager by providing the other Party with prior written notice.
- 6.5 Subcontractor - a third party to whom Service Provider has delegated or subcontracted any portion of its obligations set forth herein.
- 6.6 Work Product - All discoveries, inventions, work of authorship or trade secrets, or other intellectual property and all embodiments thereof originated by Service Provider within the scope of Services provided under this Agreement, whether or not prepared on University's premises.