Florida State University
INFORMATION SECURITY and PRIVACY
Standard Terms and Conditions

These Information Security and Privacy terms and conditions are hereby incorporated in and attached to Agreements or Contract by and between Florida State University Board of Trustees (University) and **Vendor** by reference. **Vendor** agrees to include all of the terms and conditions contained in this URL in all subcontractor or agency contracts providing services under said Contract.

Vendor acknowledges that its performance of Services under the Contract may involve access to confidential University information including, but not limited to, personally-identifiable information, student education records, protected health information, or individual financial information (collectively, "Protected or Private Information as noted in the University's Information Classification Guidelines") that is subject to state or federal law/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)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act; the Payment Card Industry Data Security Standards (PCI DSS); International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR); Federal Trade Commission Red Flags Rule and Social Security Act. **Vendor** agrees to comply with all applicable state or federal law or contract or agreements restricting the access, use and disclosure of Protected Information. **Vendor** agrees to include all of the terms and conditions contained in all subcontractor or agency contracts providing services under this Agreement.

Vendor shall not use, access, or disclose University information in any manner that would constitute a violation of state or federal law or contract or agreement terms including, without limitation, by means of outsourcing, sharing, retransfer, access, or use—to any person or entity, except:

a. Employees or agents who actually and legitimately need to access or use University Data in the performance of **Vendor's** duties under this Agreement or the Contract;

b. Such third parties, such as but not limited to, subcontractors, as may be specifically identified in this Agreement or the Contract, but only after such third party has agreed in writing and in advance of any disclosure, to be bound by all of the terms of this Agreement;

c. Any other third party approved by the University in writing and in advance of any disclosure, but only to the extent of such approval.

I. COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

With respect to the University's Protected or Private Information, and in compliance with all applicable laws and regulations, **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 (http://www.ftc.gov/reports/privacy3/fairinfo.shtm). If collecting Protected or Private Information electronically from individuals on behalf of the University, **Vendor** shall utilize a privacy statement or notice in conformance with such principles (the University's sample Privacy Statement for websites is available at http://fsu.edu/misc/policy.html).

II. PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION

Vendor agrees to hold the University's Protected or Private Information, and any information derived from such information, in strictest confidence. **Vendor** shall not access, use or disclose Protected or Private Information except as permitted or required by the Agreement or as otherwise authorized in writing by University, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected of Private Information, **Vendor** will notify University in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give University an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected or Private Information outside the United States is prohibited except on prior written authorization by the University.

III. SAFEGUARD STANDARD

Vendor agrees to protect the privacy and security of University data designated as Protected or Private Information in full compliance with any and all applicable laws, regulations, rules or standards, including, but without limitation, FERPA, HIPAA, GLB, the Federal Trade Commission Red Flags Rule, EAR, ITAR, the Social Security Act, and PCI-DSS. **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 or Private Information. While **Vendor** has responsibility for the Protected or Private 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.

- All facilities used to store and process Protected or Private 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.
- Without limiting the foregoing, **Vendor** warrants that all Protected or Private Information will be encrypted in transmission (including via web interface) and may require encrypted storage at no less than 128bit level encryption.

- **Vendor** will use industry standard and up-to-date security tools and technologies such as antivirus protections and intrusion detection methods in providing Services under this Agreement.

Vendor shall not store or process University Protected or Private Information outside of data centers located in the United States.

IV. 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 or Private Information to University in an agreed upon format, unless the University requests in writing that such data be destroyed. This provision shall also apply to all Protected or Private 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 University that such return or destruction has been completed.

V. BREACHES OF PROTECTED INFORMATION

Definition. For purposes of this article, the term, "Breach," has the meaning given to it under the applicable Florida (F.S. 501.171), applicable state or federal rule/regulation, or contractual obligation.

Reporting of Breach. Immediately upon discovery of a confirmed or suspected Breach, **Vendor** shall report both orally and in writing to the University. 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. In the event of a suspected Breach, **Vendor** shall keep the University informed regularly of the progress of its investigation until the uncertainty is resolved.

Vendor's report shall identify:

(i) The nature of the unauthorized access, use or disclosure,
(ii) The Protected or Private Information accessed, used or disclosed,
(iii) The person(s) who accessed, used and disclosed and/or received Protected or Private Information (if known),
(iv) What **Vendor** has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
(v) What corrective action **Vendor** has taken or will take to prevent future unauthorized access, use or disclosure.
(vi) **Vendor** shall provide such other information, including a written report, as reasonably requested by University.

Coordination of Breach Response Activities. In the event of a Breach, **Vendor** will:

• Immediately preserve any potential forensic evidence relating to the breach;
• Promptly (within 2 business days) designate a contact person to whom the University will direct inquiries, and who will communicate **Vendor** responses to University inquiries;
• As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore University service(s) as directed by the University, and undertake appropriate response activities;
• Provide status reports to the University on Breach response activities, either on a daily basis or a frequency approved by the University;
• Coordinate all media, law enforcement, or other Breach notifications with the University in advance of such notification(s), unless expressly prohibited by law;
• Make all reasonable efforts to assist and cooperate with the University in its Breach response efforts; and
• Ensure that knowledgeable **Vendor** staff are available on short notice, if needed, to participate in University-initiated meetings and/or conference calls regarding the Breach.

Costs Arising from Breach. In the event of a Breach by the **Vendor** or its staff, **Vendor** agrees to indemnify and hold harmless the University 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 University personnel responding to Breach, civil or criminal penalties levied against the University, attorney's fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the University.

VI. EXAMINATION OF RECORDS

University shall have reasonable access to and the right to examine any pertinent books, documents, papers, and records, regardless of the records' format, of **Vendor** involving transactions and work related to this agreement until the expiration of five years after final payment hereunder. **Vendor** shall retain project records for a period of five years from the date of final payment.

VII. 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 University at no cost to University to testify as witnesses in the event of an unauthorized disclosure caused by **Vendor** that results in litigation or administrative proceedings against University, its directors, officers, agents or employees based upon a claimed violation of laws relating to security, privacy or arising out of this agreement.

VIII. SURVIVAL

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

University Protected or Private data will include the same information security and privacy controls as the primary data center(s).

In the event of termination of the Contract, for any reason, sections V, VI, and VII shall survive for a minimum of five years from the date of such termination.

IX. RIGHT TO AUDIT

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