Recommended Contract Language for Data-Related Purchases

EXHIBIT A

SPECIAL PROVISIONS

1. PROTECTION AND HANDLING OF DATA
   a. Definitions:
      i. Institutional Data – Institutional Data is defined as data elements that are created, received, maintained and/or transmitted by the University in the course of meeting its administrative and academic requirements. Institutional Data is the property of the University and shall be managed as a key asset. It shall be managed through defined governance standards, policies, and procedures. Institutional Data is categorized in four ways: Public, Restricted, Sensitive, and Regulated.

      ii. Public – any data to which access is not restricted.

      iii. Restricted – data designated for unrestricted use within the UH community but not releasable to external parties except under the terms of a written memorandum of agreement or contract. Examples of Restricted data include, but are not limited to: student contact information (UH email address, home address, and phone number); and UH ID number (also referred to as student or employee ID number).

      iv. Sensitive – data subject to privacy considerations or classified as confidential and subject to protection from public access or inappropriate disclosure. Examples of Sensitive data include but are not limited to: date of birth; personal contact information of employees; job applicant records (names, transcripts, etc.); confidential salary and payroll information; access codes, passwords and PINs for online information systems; answers to "security questions" such as "What is the name of your favorite pet?"; confidential information subject to attorney-client privilege; detailed information about security systems (physical and/or network); and information made confidential by a collective bargaining agreement. Institutional Data not designated as Public, Restricted, or Regulated will be treated as Sensitive until a determination is made by the University or proper legal authority.

      v. Regulated – data where inadvertent disclosure or inappropriate access requires a breach notification in accordance with Hawai‘i Revised Statutes §487N or is subject to financial fines. Examples of Regulated data include but are not limited to: an individual’s first name or first initial and last name in combination with any one or more of the following: Social Security Number, driver license number or Hawai‘i ID Card number, account number, credit or debit number, access code, or

password that would permit access to an individual's financial account; Payment Card Industry Data Security Standard (PCI-DSS) information; and health information, including anything covered by the Health Insurance Portability and Accountability Act (HIPAA).

b. Data Confidentiality. Contractor shall implement appropriate measures (including written agreements signed by Contractor personnel with access to data) designed to ensure the confidentiality and security of applicable Institutional Data, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to the University or an individual identified through the data or information in the Contractor's custody, as applicable.

c. Compliance with Laws and University Policies and Procedures. Contractor agrees to comply with all applicable state and federal laws, regulations, and University policies pertaining to information designated as private, protected, sensitive or confidential by law or by the University, including, but not limited to, EP 2.210 (Use and Management of Information Technology Resources), EP 2.214 (Security and Protection of Sensitive Information), AP 7.022 (Procedures Relating to Protection of the Educational Rights and Privacy of Students), Hawai'i Revised Statutes (HRS) §487J (Social Security Number Protection), HRS §487N (Security Breach of Personal Information), HRS §487R (Destruction of Personal Information Records), and Act 10, Part V, 2008 Special Session, Session Laws of Hawai'i; the Family Educational Records Protection Act (FERPA), Health Information Privacy and Accountability Act (HIPAA), and the Gramm-Leach Bliley Act (GLBA). Contractor shall obtain and maintain all necessary permits, licenses and certificates required to provide for the delivery of service.

d. Network Security. Contractor agrees at all times to maintain network security that, at a minimum, includes: network firewall provisioning, intrusion detection, and regular (three or more annually) third party vulnerability assessments. Likewise, Contractor agrees to maintain network security that conforms to generally recognized industry standards and best practices.

e. Application Security. Contractor agrees at all times to provide, maintain and support its Software and subsequent updates, upgrades, and bug fixes such that the Software is, and remains secure from those vulnerabilities

f. Data Security. Contractor agrees to protect and maintain the security of data with protection security measures that include maintaining secure environments that are patched and up to date with all appropriate security updates as designated by a relevant authority (e.g. Microsoft notifications, etc.). Likewise Contractor agrees to conform to the following measures to protect and secure data:

    i. Data Transmission. Contractor agrees that any and all transmission or exchange of system application data with the University and other parties shall take place via secure means, e.g. HTTPS, FTPS, SFTP or equivalent means.

ii. Data Storage and Backup. Contractor agrees that any and all Institutional Data will be stored, processed, and maintained solely on designated servers and that no Institutional Data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of the Contractor designated backup and recovery processes. All servers, storage, backups, and network paths utilized in the delivery of the service shall be contained within the states, districts, and territories of the United States unless specifically agreed to in writing by an agent of the University with designated data, security, or signature authority. Contractor agrees to store all University backup data stored as part of its backup and recovery processes in encrypted form, using no less than 128 bit key.

iii. Data Re-Use. Contractor agrees that any and all Institutional Data exchanged shall be used expressly and solely for the purposes enumerated in the Agreement. UH Institutional Data shall not be distributed, repurposed or shared across other applications, environments, or business units of the Contractor. The Contractor further agrees that no Institutional Data of any kind shall be revealed, transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by a University officer with designated data, security, or signature authority.

iv. Data Encryption. Contractor agrees to store all University backup data, as applicable, as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Contractor further agrees that any and all Institutional Data defined as personally identifiable information under current legislation or regulations stored on any portable or laptop computing device or any portable storage medium is likewise encrypted.

g. PCI DSS Compliance. Contractor agrees to demonstrate compliance with PCI DSS (Payment Card Industry Data Security Standard). Contractor should be prepared to demonstrate compliance of any system or component used to process, store, or transmit cardholder data that is operated by the Contractor as part of its service. Similarly, Contractor should be prepared to demonstrate the compliance of any third party it has sub-contracted as part of the service offering. As evidence of compliance, the Contractor shall provide upon request a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor).

h. End of Agreement Data Handling. Contractor agrees that upon termination of this Agreement it shall return all Institutional Data to the University in a useable electronic form, and erase, destroy, and render unreadable all Institutional Data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities, and certify in writing that these actions have been completed within 30 days of the termination of this Agreement

or within 7 days of the request of an agent of the University, whichever shall come first.

i. Data Breach. Contractor agrees to comply with all applicable laws, including but not limited to Chapter 487N, HRS (Security Breach of Personal Information), that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of the Contractor's security obligations, or other event requiring notification under applicable law, Contractor agrees to:

   i. Notify the University by telephone and e-mail of such an event within 24 hours of discovery, and

   ii. Assume responsibility for informing all such individuals in accordance with applicable law, and

   iii. Indemnify, hold harmless and defend the University and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event, and

   iv. Assume financial responsibility for the data breach resulting from the Contractor’s negligence in handling the University’s confidential data.

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

k. Mandatory Disclosure of Protected Information. If the Contractor becomes compelled by law or regulation (including securities' laws) to disclose any non-public Institutional Data, the Contractor will provide the University with prompt written notice so that the University may seek an appropriate protective order or other remedy. If a remedy acceptable to the University is not obtained by the date that the Contractor must comply with the request, the Contractor will furnish only that portion of Institutional Data that it is legally required to furnish, and the Contractor shall require any recipient of the Institutional Data to exercise commercially reasonable efforts to keep the Institutional Data confidential.

l. Remedies for Disclosure of Confidential Information. Contractor and the University acknowledge that unauthorized disclosure or use of non-public Institutional Data may irreparably damage the University in such a way that adequate compensation could not be obtained from damages in an action at law. Accordingly, the actual or threatened unauthorized disclosure or use of any non-public Institutional Data shall give the University the right to seek injunctive relief restraining such unauthorized disclosure or use, in addition to any other remedy otherwise available (including reasonable attorneys' fees). Contractor hereby waives the posting of a bond with respect to any action for injunctive relief. Contractor further grants the University the right, but not the obligation, to enforce these provisions in the Contractor's name against any of the Contractor's

employees, officers, board members, owners, representatives, agents, contractors, and subcontractors violating the above provisions.

m. Survival. The confidentiality obligations shall survive termination of any agreement with Contractor for a period of ten (10) years or for so long as the information remains confidential, whichever is longer.