Contract Terms and Conditions for the Protection and Handling of Data
Louisiana State University
Rev. May 2018

"*Outsourced Service"* shall be defined as a technology or software infrastructure, performed function, process, or intellectual asset that is provided to LSU by a person or entity not under LSU's direct authority for a fee or as a free service.

"Protected Information" shall be defined as *data* that has been designated as private or confidential by law or by the University. *Protected Information* includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), research *data*, trade secrets, and classified government information. *Protected Information* shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any *data* constitutes *Protected Information*, the *data* in question shall be treated as *Protected Information* until a determination is made by the University or proper legal authority.

1. Data Confidentiality – Vendor shall implement appropriate measures designed to ensure the confidentiality and security of *Protected Information*, 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 with the data or information in vendor's custody.

2. Compliance with Laws and LSU Procedures – Vendor will not knowingly permit any Vendor personnel to have access to any LSU facility or any records or data of LSU if the person has been convicted of a crime in connection with

   a. a dishonest act, breach of trust, or money laundering or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, as described in Section 19 of the Federal Deposit Insurance Act, 12 U.S.C. §1829(a); or

   b. a felony.

Vendor must, to the extent permitted by law, conduct a check of public records in all of the employee's states of residence and employment for at least the last five years in order to verify the above. Vendor shall assure that all contracts with subcontractors impose these obligations on the subcontracts and shall monitor the subcontractors' compliance with such obligations. No subcontractors may be used without prior written consent of LSU.

Vendor also agrees to comply with all applicable state and federal laws, regulations, and University policies including, PS-30 (Student Privacy Rights), PS-107 (Computer User's Responsibilities), PS-114 (Security of Computing Resources), PS-06.20 (Security of Data), PS-06.25 (Privacy of Computing Resources), the Family Education Records Protection Act (FERPA), Health Information Privacy and Accountability Act (HIPPA), and the Gramm-Leach-Bliley Act (GLBA). Vendor shall obtain and maintain all necessary permits, licenses, and certificates required to provide the Outsourced Service.

3. Network Security – Vendor agrees at all times to maintain commercially reasonable network security that, at a minimum, includes: network firewall provisioning, intrusion detection/prevention, and periodic third party penetration testing. Likewise, Vendor agrees to maintain network security that at minimum conforms to one of the following:

a. Those standards that LSU is required to apply to its own network, as found at http://www.lsu.edu/it_services/its_security/it_policies/lsu-policies.php and http://www.doa.la.gov/Pages/ots/Policies.aspx

b. Current standards set forth and maintained by the National Institute of Standards and Technology, as found at https://nvd.nist.gov/ncp/repository; or

c. Any generally recognized, comparable standard that Vendor then applies to its own network (e.g. ISO 27002) and which has been approved in writing by LSU.

4. Data Security – Vendor 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, Vendor agrees to conform to the following measures to protect and secure data:

a. Data Transmission – Vendor agrees that any and all transmission or exchange of system application data with LSU and/or any other parties, solely in accordance with Section 6 below, shall take place via secure means, e.g. HTTPS, FTPS, SFTP, or equivalent means.

b. Data Storage and Backup – Vendor agrees that any and all LSU data will be stored, processed, and maintained solely on designated servers and that no LSU 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 Vendor's 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 LSU officer with designated data, security, or signature authority. An appropriate officer with the necessary authority can be identified by the LSU Chief Information Security Officer for any general or specific case.

   Vendor agrees to store all LSU backup data as part of its backup and recovery processes in encrypted form, using no less than 128 bit key.

c. Data Re-use – Vendor agrees that any and all data exchanged shall be used expressly and solely for the purposes of enumerated in the Agreement. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of Vendor. As required by Federal law, Vendor further agrees that no LSU 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 an LSU officer with designated data, security, or signature authority.

5. Compliance – Vendor agrees to periodically demonstrate compliance with PCI DSS (Payment Card Industry Data Security Standard). Vendor should be prepared to demonstrate compliance of any system or component used to process, store, or transmit cardholder data that is operated by the Vendor as part of its service. Similarly, Vendor 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 Vendor shall provide upon request a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor).

6. End of Agreement Data Handling – Vendor agrees that upon termination of the Agreement, it shall return all data to LSU in a useable electronic form, and erase, destroy, and render unreadable all LSU 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 LSU, whichever shall come first.

7. Data Breach – Vendor agrees to comply with the Louisiana Database Breach Notification Law (Act 499) (https://legis.la.gov/Legis/Law.aspx?d=322027), and all applicable laws 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 Vendor's security obligations or other event requiring notification under applicable law ("Notification Event"), Vendor agrees to notify LSU immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend LSU and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification event.

8. Right to Audit – Vendor agrees that, as required by applicable state and federal law, auditors from state, federal, LSU System, 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 or the University during normal working hours for this purpose.

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

10. Remedies for Disclosure of Confidential Information – Vendor and LSU acknowledge that unauthorized disclosure or use of the *Protected Information* may irreparably damage LSU 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 *Protected Information* shall give LSU the right to seek injunctive relief restraining such unauthorized disclosure or use, in addition to any other remedy otherwise available (including reasonable attorneys' fees). Vendor hereby waives the posting of a bond with respect to any action for

injunctive relief. Vendor further grants LSU the right, but not the obligation, to enforce these provisions in Vendor's name against any Vendor's employees, officers, board members, owners, representatives, agents, contractors, and subcontractors violating the above provisions.

11. Safekeeping and Security – as part of the *Outsourced Service*, Vendor will be responsible for safekeeping all keys, access codes, combinations, access cards, personal identification numbers and similar security codes and identifiers issued to Vendor's employees, agents, contractors, or subcontractors. Vendor agrees to requires its employees to promptly report a lost or stolen device or information.

12. Non-Disclosure – Vendor is permitted to disclose Confidential Information to its employees, authorized contractors and subcontractors, agents, consultants, and auditors on a need to know basis only, provided that all such contractors, subcontractors, agents, consultants and auditors have written confidentiality obligation to Vendor and LSU.

13. Request for Additional Protection – From time to time, LSU may reasonably request that Vendor protect the confidentiality of certain *Protected Information* in particular ways to ensure that confidentiality is maintained. Vendor has the right to reasonably decline LSU's request. In the event that such a request requires Vendor to take steps beyond those otherwise by Section 9 in order for Vendor to comply, Vendor shall notify LSU as to the cost of compliance and LSU may thereafter, in its sole discretion, direct Vendor to take such steps.

14. Survival – The confidentiality obligations shall survive termination of any agreement with Vendor a for a period of ten (10) years or for so long as the information remains confidential, whichever is longer and will inure to the benefit of LSU.