Data Security Rider

Effective Date: 08/24/2016

Background: This contract rider must be added to all contracts with any service provider (also known as "vendor"), if the service provider, in connection with its services; maintains, processes, hosts or otherwise manages; or takes custody of, stores, or otherwise has access to and use of University of Cincinnati (also known as "university"), faculty or student data. The service provider agrees to the terms of this contract rider. The intent of this contract rider is to make clear the information security requirements the university demands from all service providers.

Security Standards: All the service provider's systems handling university data must comply with the university's minimum safeguards as defined by the university's Data Governance and Classification Policy. All systems and applications shall regularly undergo vulnerability assessments, such as testing patch level, password security, and application security. Routine event monitoring will be performed by the service provider; the university expects the service provider will routinely and immediately identify events related to unauthorized activity and unauthorized access. The service provider should undergo regular security audits, preferably by certified third parties, occurring at least annually, and any identified issues must be resolved within 90 days of the audit report. The university may demand written proof of this audit at any time during the term of the contract. All services gathering restricted data as defined by the university's Data Governance and Classification Policy must utilize secure communication methods, such as SSL, and use a certificate from an approved independent authority. All file transmissions involving restricted data or otherwise sensitive data as defined by the university must utilize secure communication methods; for example, SSL, SSH, SFTP.

Definition: ***Covered data and information (CDI)*** includes paper and electronic data classified as "Restricted" by the university's Data Governance and Classification Policy. This includes information supplied by university, as well as any data provided by university's students to the service provider. Service provider agrees to follow all requirements as defined in the university's Data Governance and Classification Policy.

Physical Access to CDI: Physical access to facilities where data are stored, whether production or backup, must reside within the continental United States. Any damage or unauthorized access to facilities must be reported to university within twenty-four hours of its discovery. If any unauthorized access to university data occurred, the service provider must consult with university officials before notifying those affected by the unauthorized access.

Acknowledgment of Access to CDI: Service provider acknowledges that the Agreement allows the service provider access to CDI. Data access shall be limited to those with a "need to know" and controlled by specific individual(s). At no time will university data be physically or logically accessible to a foreign national. The service provider must have procedures and solutions implemented to prevent unauthorized access, and the procedures will be documented and available for university to review upon request. All of the service provider's employees with access to university data must be identified with names provided to the university upon request.

Prohibition on Unauthorized Use or Disclosure of CDI: Service provider agrees to hold CDI in strict confidence. Service provider shall not use or disclose CDI received from or on behalf of university (or its students) except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by university. Service provider agrees not to use CDI for any purpose other than the purpose for which the disclosure was made.

Retention, Return or Destruction of CDI: Upon termination, cancellation, expiration or other conclusion of the Agreement, service provider shall return all CDI to university or, if return is not feasible, destroy any and all CDI. Destruction of CDI shall be carried out in accordance with university's data retention policies. The university shall approve the method of data destruction prior to destruction. If the service provider destroys the information, the service provider shall provide university with a certificate confirming the date and method of destruction of the data.

Remedies: If the university reasonably determines in good faith that service provider has materially breached any of its obligations under this contract, the university, in its sole discretion, shall have the right to require service provider to submit to a plan of monitoring and reporting; provide service provider with a fifteen (15) day period to cure the breach; or terminate the agreement immediately if cure is not possible. Before exercising any of these options, university shall provide written notice to service provider describing the violation and the action it intends to take.

Maintenance of the Security of Electronic Information: Service provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from, or on behalf of university or its students. These measures will be extended by contract to all subcontractors used by service provider.

Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service provider shall, within one day of discovery, report to university any use or disclosure of CDI not authorized by this agreement or in writing by university. Service provider's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the CDI used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what service provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action service provider has taken or shall take to prevent future similar unauthorized use or disclosure. Service provider shall provide such other information, including a written report, as reasonably requested by university.

Authentication: Service provider agrees to allow the use of Shibboleth authentication (or comparable authentication mechanism with university approval) if and when appropriate as requested by the university.

Vulnerability Scanning: Service provider agrees to allow university to perform regular pen testing/vulnerability scans (operating system, patch, and application).

System Logs: Service provider shall agree to forward unmodified system (and other appropriate) logs to university owned SIEM (Security Information and Event Management) system owned by IT@UC Office of Information Security.

Compliance: Service provider must supply documentation of compliance with any applicable laws and regulations.

Note: Inclusion of data provided by students into the terms of the contract will depend upon the contract and may not be needed.

Addendums
The service provider agrees to the riders below that are checked.

☐ **PCI DSS**: For credit card transactions processed via a network-based service, the service provider must supply evidence of Payment Card Industry Data Security (**PCI DSS)** compliance. Credit card numbers shall not be stored unless the university has approved a retention period for storage in advance. Credit card numbers will be encrypted when stored and transmitted, and masked on displays and reports.

☐ **GLBA**: For financial records processing, the service provider shall supply documentation of compliance with Gramm-Leach-Bliley Act (**GLBA**) prior to the contract being accepted by the university, and annually thereafter. All payment processing must comply with university financial policy(s).

☐ **Personally Identifiable Health Information (PIHI)**, whether or not protected by the Health Insurance Portability and Accountability Act (HIPAA), must be encrypted if stored in electronic format. Protected Health Information (PHI) requires a Business Associate Agreement to be in place.

☐ **FERPA**: Service provider agrees to abide by the limitations on re-disclosure of personally identifiable information from education records set forth in The Family Educational Rights and Privacy Act (**FERPA**) (34 CFR § 99.33 (a)(2)) and with the terms set forth below. 34 CFR 99.33 (a)(2) states that the officers, employees and agents of a party that receives education record information from the university may use the information, but only for the purposes for which the disclosure was made. Service provider shall supply documentation of compliance with FERPA prior to execution of the contract and annually thereafter. If the Family Policy Compliance Office of the U.S. Department of Education determines that the service provider improperly disclosed personally identifiable information obtained from university's education records, university may not allow the service provider access to education records for at least five years.

Last Updated: 8/24/2016