*Contract Addendum for External Data and Systems Service Providers (Appendix 4)*

Version 02/09/2018, Chief Data Officer

**Authorization:**

* This template is known as Appendix 4 to Policy [UNIV 1.52, Responsible Use of Data, Technology and User Credentials](https://emailsc-my.sharepoint.com/personal/kellymc2_mailbox_sc_edu/Documents/CDO/DataGov/sc.edu/policies/ppm/univ152.pdf)
* See also [UNIV 1.51, Data & Information Governance](https://emailsc-my.sharepoint.com/personal/kellymc2_mailbox_sc_edu/Documents/CDO/DataGov/sc.edu/policies/ppm/univ151.pdf)

**UNIV 1.52 ¶ II.A.5 (Procedures for All Campuses)**

University employees purchasing or acquiring data and/or technology services, systems, and software are responsible for establishing a *Contract Addendum for External Data and Systems Service Providers* with vendors prior to initiating services (Appendix 4). Such acquisitions may include hosted services from a third party which involve university data or business processes, as well as services through which Constituents submit their personal data to the vendor or service provider. The Contract Addendum must be included with solicitations, RFPs, contract approvals, and procurement documentation.

*Justification*

This agreement supports State of South Carolina, Division of Information Security, *Security and Compliance Controls SCDIS-200-2.211, 8.102 and 12.405*, effective for state agencies July 2016.

The content below is a model contract Addendum for USC organization units to include with any Invitation for Bids (IFB), Request for Proposal (RFP), or other formal solicitation documents and procurement/purchasing for services, software, and systems that include Covered Data and Information (CDI, as defined below). This template may be modified in consultation with appropriate university officials, including but not limited to General Counsel, Purchasing, Chief Data Officer, Chief Information Security Officer, and Data Stewards of included data and information. *If CDI is not involved, then this Addendum is not necessary.*

*Responsibility for Implementation*

University employees contracting to purchase or otherwise acquire services, systems, and software, including hosted services, which involve university data or business processes are responsible for ensuring this contract addendum is incorporated into the contract between the university and the vendor.

University Purchasing will facilitate the inclusion of a completed version of this template in solicitations under Section 7B, Special Terms and Conditions; if there are questions about applicability to a particular procurement, the Chief Data Officer, Chief Information Security Officer, Procurement Officer, and/or General Counsel may be consulted.

This template is intended to fulfill, but not necessarily replace, provisions of the State Fiscal Accountability Authority (SFAA) Procurement Compendium, Version 2.0.2 (September 2017; see <https://procurement.sc.gov/legal/proc-docs> ), including but not limited to clauses pertaining to Information Security (inclusive of 7B104-1, 7B105-1, 7B106-1), Information Use and Disclosure (7B108-1 and 7B110-1), and Ownership of Data and Materials (7B125-1). A Service Provider Security Assessment Questionnaire (04-4027-1), Contractor’s Liability Insurance – Information Security and Privacy (7B058-1), and Subcontractor Identification (5030-2) may also be recommended or required.

Note: This Addendum should be used only in conjunction with a contract between the university and a third party. If the university intends to share CDI with a third party but no formal agreement exists between the parties, then please refer to Appendix 3 of Policy UNIV 1.52.

*Explanations, Adjustments, and Revisions*

Applicable sections of the following verbiage may be included in contract documents, where appropriate.  The Office of General Counsel and the Data Steward(s) of the particular university data involved in the related Agreement will assist in explaining and/or negotiating terms of this Addendum with the Service Provider.

*Remove all content above before presenting to Service Provider for completion & signature*

**CONTRACT ADDENDUM FOR**

**EXTERNAL DATA & SYSTEMS SERVICE PROVIDERS**

This document constitutes an Addendum to the Agreement dated \_\_\_\_\_\_ between the University of South Carolina (hereinafter "Institution") and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter "Service Provider"). If any of the terms of this Addendum conflict with any of the terms of the Agreement, then the terms of this Addendum shall control.

**Protection of Covered Data** **and Information**

Service Provider agrees to abide by limitations binding upon the Institution and related to the transmission, storage, access, analysis, and/or disclosure of Covered Data and Information (CDI); this includesvarious federal and state legislation, regulations, policies, and industry practices.

**Definition: Covered Data and Information (CDI)** includes Personally Identifiable Information (PII) concerning university Constituents, as well as University Data, as defined in [UNIV 1.51](http://www.sc.edu/policies/ppm/univ151.pdf), and may include paper records, electronic images, data and other information records supplied by Institution, as well as paper records, electronic images, data and other information records the Institution’s Constituents provide directly to the Service Provider. Data classified by university Data Stewards as Restricted or Confidential is considered CDI unless specifically exempted by this Addendum. A list of potentially applicable items is located in Enterprise Data Standard 1.04 (Data Classification Level and Potentially Applicable Data Items; see <http://www.sc.edu/about/offices_and_divisions/division_of_information_technology/docs/dataclassificationschema_eds104.pdf> ).

**Definition: Constituents** are persons and entities that have a relationship to any organizational unit of the university system, including but not limited to: students (prospective students, applicants for admission, enrolled students, campus residents, former students, and alumni), employees (faculty, staff, administrators, student employees, prospective employees, candidates for employment, former employees and retirees), and other affiliates (including but not limited to board members, consultants, contractors, donors, invited guests, recipients of goods and services, research subjects, and volunteers).

**Data Inventory:** Prior to any transaction of data and information, including but not limited to CDI, the Institution and Service Provider must document the inventory of data elements proposed for transmission, storage, access, or other disclosure. Per university policy [UNIV 1.52](https://emailsc-my.sharepoint.com/personal/kellymc2_mailbox_sc_edu/Documents/CDO/DataGov/sc.edu/policies/ppm/univ152.pdf), and state of SC regulations on information privacy (especially SC DIS-200) the data elements must be properly classified and permitted for transaction by the appropriate Data Steward. The University Information Security Office (UISO) will review any Agreement that includes Restricted or Confidential data. If PII is involved, procedures related to and include a Privacy Impact Assessment must be completed prior to transaction, and are subject to review by the Institution’s Chief Privacy Officer. Mitigation strategies may be recommended or required by the UISO or Chief Privacy Officer. The data inventory, approval, and recommendations or requirements shall become an artifact in the Statement of Work (or similar) in the Agreement. Under exceptional circumstances, should the parties be unable to mutually agree to a data inventory under the Agreement, the Agreement may be terminated.

**Acknowledgment of Access to CDI:** Service Provider acknowledges that the Agreement allows the Service Provider and Institution to mutually transmit, store, and access CDI.

**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 Institution (or its Constituents) except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by Institution. Service Provider agrees not to access or use CDI for any purpose other than the purpose for which the disclosure was made.

**Return or Destruction of CDI:** Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall return all CDI to Institution or, if return is not feasible, destroy any and all institutional CDI. If the Service Provider destroys the information, the Service Provider shall provide Institution with a certificate confirming the date of destruction of the data.

**Remedies:** If Institution reasonably determines in good faith that Service Provider has materially breached any of its obligations under the Agreement, then Institution, in its sole discretion, shall have the right to (1) require Service Provider to submit to a plan of monitoring and reporting, (2) provide Service Provider with a fifteen (15) day period to cure the breach, or (3) terminate this Agreement immediately if cure is not possible. Before exercising any of these options, Institution 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 transmitted and stored CDI received from, or on behalf of Institution or its Constituents. Service Provider shall impose these measures on all subcontractors used by Service Provider.

**Reporting Unauthorized Disclosures or Misuse of Covered Data and Information:** Service Provider shall, within one (1) day of discovery, report to Institution any use or disclosure of CDI not authorized by the Agreement or in writing by Institution. Service Provider's report shall identify: (1) the nature of the unauthorized use or disclosure, (2) the CDI used or disclosed, (3) the identity of the individual(s) or entity that received the unauthorized disclosure, (4) the action(s) that Service Provider has taken or shall take to mitigate any potentially negative effects of the unauthorized use or disclosure, and (5) the corrective action(s) Service Provider has taken or shall take to prevent future similar unauthorized uses or disclosures. Service Provider shall provide any additional information in connection with the unauthorized disclosure reasonably requested by Institution.

**Indemnification:** Service Provider shall indemnify, save and hold harmless Institution from any loss, liability, damage, claims, costs or judgments the Institution incurs, including Institution's costs and attorney fees, which arise from Service Provider's failure to meet any of its obligations under the Agreement, including but not limited to this Addendum.