*External Data and Information Sharing Certification (Appendix 3)*

Version 02/09/2018, Chief Data Officer

**Authorization:**

* This template is known as Appendix 3 to University Policy [UNIV 1.52, Responsible Use of Data, Technology and User Credentials](http://www.sc.edu/policies/ppm/univ152.pdf)
* See also [UNIV 1.51, Data & Information Governance](http://www.sc.edu/policies/ppm/univ151.pdf)

**UNIV 1.52 ¶ II.A.4 (Procedures for All Campuses)**

University personnel responsible for sharing or transmitting university data or information concerning university Constituents, operations, or business processes with an external entity are responsible for ensuring an External Data and Information Sharing Certification is executed prior to any sharing or transmission (Appendix 3).

*Justification*

This document 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 template is a model certification that external organizations that receive and/or utilize University Covered Data and Information (CDI), as defined below, should execute. The certification is required absent a contract between the University and the receiving external organization. This template may be modified in consultation with appropriate university officials, including but not limited to General Counsel, the Chief Data Officer, the Chief Information Security Officer, and Data Stewards of included data and information. *If CDI is not involved, then this certification is not necessary.*

*Responsibility for Implementation*

University employees who are responsible for sharing or transmitting University Data or information concerning university Constituents with PII, or non-person data classified as Restricted or Confidential, with an external entity are responsible for ensuring this Certification is executed prior to any sharing or transmission. Note: if procurement, purchasing, or other form of contract is involved, this form should not be used; instead please refer to Template - Contract Addendum for External Data & Systems Service Providers (Appendix 4).

*Explanations, Adjustments, and Revisions*

Data Stewards of the particular University Data or information may adjust the template to serve their needs. The Office of General Counsel and the Chief Data Officer/Agency Privacy Liaison will assist in explaining and/or negotiating terms of this Certification with the Receiving Entity.

*Remove all content above before presenting to Receiving Entity for completion*

**CERTIFICATION OF EXTERNAL ENTITY** **RECEIVING**

**UNIVERSITY OF SOUTH CAROLINA COVERED DATA AND INFORMATION**

**Purpose/Reason(s) for Sharing**

[detailed purpose/reason/benefit/need/requirement of the Receiving Entity for the requested information, including applicable research study name, legislation, regulation, compliance obligation, or other justification or requirement]

**Source & System**

[name the specific organizational unit and the source data store or system from which records will be shared]

**Data Elements**

[provide detailed list of data elements proposed for exchange and their Data Classification]

|  |  |  |
| --- | --- | --- |
| Data Element | Data Classification | Business need/justification  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

 <<insert additional rows as needed>>

The data or information shared under this Certification ⬜ includes or ⬜ does not include Personally Identifying Information, as defined by South Carolina statutory law, S.C. Code Ann. § 16-13-510(D), <http://www.scstatehouse.gov/code/t16c013.php> or other data and information classified as Restricted or Confidential.

If person records are included in the shared data, the Data Element to be included to ensure accurate identification of unique persons (also known as a unique personal identifier) is: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Frequency of Sharing**

[describe how often the data is to be provided and/or refreshed]

**Sharing Lifecycle**

This agreement begins on [begin date] and terminates on [end date]. [Add any other date/time conditions or limitations for use of data & information.]

**Ownership of Data and Information**

The university retains exclusive rights to all data, content, and information the university collects, produces, transmits, and stores regarding its Constituents, services, programs, and operations.

**Protection of Covered Data and Information**

Receiving Entity agrees to abide by limitations binding upon USC related to the transmission, storage, access, and 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 Identifying Information (PII) concerning university Constituents, as well as University Data, as defined in UNIV 1.51, and may include paper records, electronic images, data and other information records supplied by USC, as well as paper records, electronic images, data and other information records USC’s Constituents provide directly to the Receiving Entity. Data classified by university Data Stewards as Restricted or Confidential is considered CDI unless specifically exempted by this Certification. 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).

**Acknowledgment of Access to CDI:** Receiving Entity acknowledges that this Certification allows the Receiving Entity and USC to mutually transmit, store, and access CDI.

**Prohibition on Unauthorized Use or Disclosure of CDI:** Receiving Entity agrees to hold CDI in strict confidence. Receiving Entity shall not use or disclose CDI received from or on behalf of USC (or its Constituents) except as permitted or required by the Certification, as required by law, or as otherwise authorized in writing by USC. Receiving Entity 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:** Receiving Entity shall return all CDI to USC or, if return is not feasible, destroy any and all CDI once the Receiving Entity no longer requires the CDI. If the Receiving Entity destroys the information, then the Receiving Entity shall provide USC with a certificate confirming the date of destruction of the CDI.

**Remedies:** If USC reasonably determines that Receiving Entity has materially breached any of its obligations under this Certification, then USC, in its sole discretion, shall have the right to (1) require Receiving Entity to submit to a plan of monitoring and reporting, (2) provide Receiving Entity with a fifteen (15) day period to cure the breach, or (3) require the Receiving Entity to return to USC or destroy all CDI if cure is not possible.

**Maintenance of the Security of Electronic Information:** Receiving Entity 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 USC or its Constituents. Receiving Entity shall impose these measures on all subcontractors used by Receiving Entity.

**Reporting Unauthorized Disclosures or Misuse of Covered Data and Information:** Receiving Entity shall, within one (1) day of discovery, report to USC any use or disclosure of CDI not authorized by the Certification or in writing by USC. Receiving Entity'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 Receiving Entity has taken or shall take to mitigate any potentially negative effects of the unauthorized use or disclosure, and (5) the corrective action(s) Receiving Entity has taken or shall take to prevent future similar unauthorized uses or disclosures. Receiving Entity shall provide any additional information in connection with the unauthorized disclosure reasonably requested by USC.

**USC Designated Point of Contact**

 [Name]

 [Position or Job Title]

 [Organizational Unit]

 [Work Phone]

 [USC-issued Email Address]

In the event the above-named contact is unavailable or cannot be reached, the alternate contact is:

 [Name or Office]

 [Phone Number]

**Receiving Entity’s Authorized Representative**

 [Full Legal Name]

 [Position or Title]

 [Phone Number]

 [Email Address]

 [Full Mailing Address]

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Signature Date