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

*[Appropriate when transmitting or sharing university data with an external entity]*

Version 12/07/2021, Data Stewardship Program Manager

**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*

The Data Steward for an organizational unit that is requested to share the data or information (the ‘Sender’) is responsible for ensuring this agreement is executed prior to any sharing or transmission and has both the responsibility and authority to approve data sharing. The Data Steward is entitled and expected to request and receive full, complete, and accurate information about how the requested data will be used, and may require additional responses, documentation about architecture, security, and privacy, or other responses/attestations to support the request. The submission of a request does not ensure its approval.

Note: if procurement, purchasing, or other form of contract is involved, please refer to Template - Contract Addendum for External Data & Systems Service Providers (Appendix 4). This form can be used in conjunction with the Contract Addendum.

To identify the appropriate Data Steward for the data, please see <https://sc.edu/about/offices_and_divisions/division_of_information_technology/chiefdataofficer/data_stewardship/datastewardroster.php>

*Explanations, Adjustments, and Revisions*

This template may be modified by Data Stewards. As needed, Data Stewards should consult other university officials, including but not limited to General Counsel, the Chief Data Officer, Data Steward Program Manager, Agency Privacy Liaison (Office of General Counsel), the Chief Information Security Officer, and other Data Stewards of included data and information.

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.

When requesting Student Data from Banner, requesting party must also complete a formal request through the Data Access Permissions System (DAPS, <https://www.sc.edu/daps/>) and associated requirements. This agreement may be uploaded with a DAPS request.

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

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

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

This document constitutes a Data Sharing Agreement for the purpose of sharing data between a subunit of the University of South Carolina (UofSC) and an external entity.

The requestor is \_\_\_\_\_\_\_\_\_\_\_\_­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (UofSC organizational unit) \_.

The external recipient (receiving entity) is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the external entity) \_.

The data steward(s) for the data is/are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(data owner(s) for the data elements being shared) \_.

Listed Data Stewards: <https://sc.edu/about/offices_and_divisions/division_of_information_technology/chiefdataofficer/data_stewardship/datastewardroster.php>

Any questions or assistance needed in filling out this agreement can be directed to the Data Steward Program Manager, Sue Porter, at porters@mailbox.sc.edu.

If any of the terms of this Agreement conflict with any of the terms of other formal agreements binding the above-named parties, the terms of this official agreement will control.

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

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

When driven by an external contract, law, or regulation, please cite the corresponding contract number or legal reference information.]

**Source & System(s)**

[Name the specific organizational unit and the source data store or system from which records will be shared. If there are multiple sources, please name all and designate which system supplies each data element.]

**Data Elements**

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

If sourced from multiple operational units, please add a column for responsible data steward.]

|  |  |  |
| --- | --- | --- |
| **Data Element** | **Data Classification** | **Source System (if multiple sources)** |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |
|  | Choose an item. |  |

 <<insert additional rows as needed>>

**Data Sharing Details**

**Destination System and/or Use**

[name and description of information store or system that will receive/import/integrate the data at the Recipient organizational unit]

**Method of Sharing**

[describe the physical, technical, or other manner in which data or information will be shared between the organizational units. If data will be exchanged bi-directionally, describe in detail.]

**Resource Account**

If the method of sharing is an integration or interface that requires a resource account, complete the following:

Resource account name: [Name]

Approving parties: [List]

Date authorized: [Date]

**Frequency of Sharing**

[Describe how often the data is to be provided and/or refreshed, up to and including ‘real-time integration].

 (Will there be an initial feed of data to seed the external system? If so, how often will that be updated?)]

**Sharing Lifecycle**

This agreement begins on [begin date (first day of the following month)] and terminates on [end date (one year after the begin date)]. [Add any other date/time conditions or limitations for use of data & information.] Note: the external agreements must be reviewed and/or renewed each year, or more frequently, if significant changes occur.

**Selection Criteria for Included Records**

USC adheres to the principle of least privilege, meaning that recipients of data and information should receive no more information than is absolutely required in order to complete an assigned job or responsibility.

[describe the selection criteria for records to be shared; consider criteria such as: ‘students majoring in a particular academic program,’ or ‘former employees who retired during the 2015 calendar year.’]

**Person Records**

The data or information shared under this Agreement

[ ]  includes PII

[ ]  does not include PII

**Personal Identifying Information (PII),**

as defined by South Carolina statutory law, S.C. Code Ann. § 16-13-510(D), <http://www.scstatehouse.gov/code/t16c013.php>, or

as defined by the State of South Carolina Data Breach Law, *see SECTION 39-1-90 (D.3.),* [*http://www.scstatehouse.gov/code/t39c001.*php](http://www.scstatehouse.gov/code/t39c001.php), or

other data and information classified as Restricted or Confidential.

(Keep in mind that if multiple data elements are being shared, their combined classification could be more restrictive than any of the elements individually.)

If person records are included, the Data Element(s) that ensures accurate identification of unique persons is known as a unique personal identifier. Please list below.

Unique Personal Identifier is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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**

Recipient agrees to abide by limitations binding upon the UofSC and related to the transmission, storage, access, and disclosure of Personally Identifiable Information from Covered Data and Information records; this includesvarious federal and state legislation, regulations, policies, and industry practices.  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: 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 UofSC, as well as paper records, electronic images, data and other information records UofSC’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 UofSC (or its Constituents) except as permitted or required by the Certification, as required by law, or as otherwise authorized in writing by UofSC. Receiving Entity agrees not to access or use CDI for any purpose other than the purpose for which the disclosure was made.

**Additional Restrictions or Parameters:**

[Sender / Data Steward stipulates the following additional restrictions or parameters.]

**Return or Destruction of CDI:** Receiving Entity shall return all CDI to UofSC 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 UofSC with a certificate confirming the date of destruction of the CDI.

**Remedies:** If UofSC reasonably determines that Receiving Entity has materially breached any of its obligations under this Certification, then UofSC, 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 UofSC 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 UofSC any use or disclosure of CDI not authorized by the Certification or in writing by UofSC. 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 UofSC.

**Requirements for Documentation, Review and Data Definitions**

Once finalized, this Data Sharing Agreement must be registered with DoIT Analytics and Data Governance and scheduled for annual review, leading to renewal, alteration, or elimination. To initiate a request, the Requestor must submit a Service Desk ticket under the catalog item ‘Data Governance’ or by clicking [this link](https://scprod.service-now.com/sp?id=sc_cat_item&sys_id=df407b46130c27003f0f50782244b022).

Data elements flowing from the Sender to the Requestor must be defined and classified with Data Analytics and Governance to fully support and document this agreement.

The Requestor is likewise responsible for defining the universe of data elements contained in the receiving information system or data store with Data Analytics and Governance.

**Electronic Signature and Acceptance**

The completion of the following information signifies acknowledgement and acceptance of all above provisions and responsibilities. Automated approval in the document module of ServiceNow can be substituted for actual signatures of the requestor and data steward(s) below. The external recipient will still need either a signature or a copy of an email agreeing to the provisions and responsibilities.

**The Requestor’s designated Point of Contact** and signature for this Agreement is:

 [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]

**The Requestor’s Electronic Signature and Acceptance**

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

Signature Date

**External Recipient’s Authorized Representative**

 [Full Legal Name]

 [Position or Title]

 [Phone Number]

 [Email Address]

 [Full Mailing Address]

**The External Recipient’s Electronic Signature and Acceptance**

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

Signature Date

**The Data Steward(s) / Sender(s)** for this Agreement is: (If more than one, please repeat this section.)

 [Name]

 [Position or Job Title]

 [Work Phone]

 [USC-issued Email Address]

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

 [Name and Job Title]

 [Published Phone Number]

This Data Sharing Agreement is:

⬜ approved

⬜ denied pending further information

⬜ denied and ineligible for reconsideration

⬜ scheduled for termination on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

⬜ other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The Data Steward’s Electronic Signature and Acceptance (if different from requestor)**

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

Signature Date

<< For multiple data stewards, include additional names and signatures here: >>