Internal Data and Information Sharing Agreement (Appendix 2)

Version 06/30/2021, Data Steward Program Manager

Authorization:

- This template is known as Appendix 2 to Policy UNIV 1.52, Responsible Use of Data, Technology and User Credentials
- See also UNIV 1.51, Data & Information Governance

UNIV 1.52 ¶ II.A.3 (Procedures for All Campuses)

> University organizational units that require internal exchange, transmission, or other sharing of data and information must establish and adhere to an Internal Data and Information Sharing Agreement (Appendix 2) prior to any sharing or transmission.

Justification

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

The intent of an internal data sharing agreement is to specify the specific need and parameters of data sharing, including placing limits on the recipient for not further sharing data and information they receive. Appendix 2 applies to transmission/sharing of large sets of unit records to seed or sync information systems and databases, where the unit records qualify as University Data or Personally Identifiable Information (per UNIV 1.51); incidental and smaller internal transmissions for purposes of information, reporting, and analysis are covered by User Agreements (Appendix 1).

An internal agreement is not necessary for content with Data Classification of Public Information, is advisable for assets or data classified as Internal Use and must be included for assets and data classified as Confidential and/or Restricted.

The content below represents a model agreement that USC organizational units should negotiate and employ with other internal organizational units that receive and/or utilize University Data or information. The sharing may take the form of file transmission over network or via hardware, through systems integration or interface, including scheduled jobs executed by Division of Information Technology (DoIT).

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.

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.

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 Recipient for completion

---

INTERNAL DATA AND INFORMATION SHARING AGREEMENT

UNIVERSITY OF SOUTH CAROLINA

This document constitutes a Data Sharing Agreement between two or more organizational units of the University of South Carolina (UofSC).

The requestor/recipient is ___________________________ (UofSC organizational unit).
The sender/supplier is __________________________ (UofSC organizational unit) .
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]
Any restricted or confidential data elements require individual business case justification

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 internal 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 that is absolutely required in order to complete an assigned job or responsibility.
[describe the selection criteria for records to be shared; give full consideration to 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, 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

Per policy UNIV 1.51 (Data and Information Governance) the Sender 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 includes various 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).

Prohibition on Unauthorized Use or Disclosure of CDI: Recipient agrees to hold CDI in strict confidence. Recipient shall not use or disclose CDI received from or on behalf of Sender (or its Constituents) except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing. Recipient agrees not to access or use CDI for any purpose other than the Purpose for which the sharing agreement was made, as stated above, or here:

Additional Restrictions or Parameters:
[Sender / Data Steward stipulates the following additional restrictions or parameters.]

Return or Destruction of CDI: Upon termination, cancellation, expiration or other conclusion of the Agreement, Recipient shall return all CDI to Sender or, if return is not feasible, destroy any and all CDI. If the Recipient destroys the information, the Recipient shall provide Sender with a formal notice confirming the date of destruction.

Remedies: If Sender reasonably determines in good faith that Recipient has materially breached any of its obligations under the Agreement, then Sender shall have the right to (1) require Recipient to submit to a plan of monitoring and reporting, (2) provide Recipient with a fifteen (15) day period to cure the breach, or (3) terminate the Agreement immediately if cure is not possible. Before exercising any of these options, Sender shall provide written notice to Recipient describing the violation and the action it intends to take.

Maintenance of the Security of Electronic Information: Recipient 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. Recipient shall impose these measures on all subcontractors or other third parties used by Recipient.

Reporting Unauthorized Disclosures or Misuse of Covered Data and Information: Recipient shall, within one (1) day of discovery, report to Sender, the University Information Security Office (UISO), and Agency Privacy Liaison any use or disclosure of CDI not authorized by the Agreement or in writing. Recipient'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 Recipient has taken or shall take to mitigate any potentially negative effects of the unauthorized use or disclosure, and (5) the corrective action(s) Recipient has taken or shall take to prevent future similar unauthorized uses or disclosures. Recipient shall provide any additional information in connection with the unauthorized disclosure reasonably requested by Sender or UISO.

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.

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.

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

The Sender's designated Point of Contact (if different from the Data Steward) for this Agreement and related provisions is:

[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]

The Data Steward(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 sender)

_______________________________________ _______________________________
Signature Date

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