NUMBER:	UNIV 1.52 (NEW)
SECTION:	University Administration
SUBJECT:	Responsible Use of Data, Technology, and User Credentials
DATE:	June 30, 2016
Policy for:	All Campuses
Procedure for:	All Campuses
Authorized by:	President
Issued by:	President's Office

I. Policy

All individuals and organizational units that use or access university data, technology, and user credentials must comply with state and federal laws, statutes, and regulations; must comply with all applicable university policies, standards, and procedures; must have prior authorization for related activities based on job duties or other demonstrated need, and must not compromise the appropriate availability, confidentiality, integrity, privacy, or security of data, technology, and user credentials.

In order to successfully carry out its mission, USC will act to protect the confidentiality, integrity, and availability of data, technology, and user credentials. USC promotes responsible use and prohibits unauthorized use of these university assets, including for personal or other non-university purposes. Such use may be grounds for investigation and disciplinary action.

A. Policy Statement

1. The university retains all rights to its data, technology, and user credentials.

2. The university utilizes the State of South Carolina definition of Personal Identifying Information (PII) and affords protections to such information accordingly.

3. The university promotes the Principle of Least Privilege (POLP) by limiting access to its assets based on job duties or other demonstrated need.

4. All users have a direct personal responsibility for the appropriate use of university data, technology, and user credentials; all users must comply with this policy and related standards and procedures, and must:
    a. protect and properly use these assets regardless of their physical location;
    b. adhere to applicable state and federal laws, statutes, and regulations;
    c. abide by USC policies, procedures, guidelines, and privacy and security protections and controls;

d. accept responsibility for all activity initiated or conducted through the use of their user credentials;
e. refrain from accessing or using university Data and Information for Personal Matters;
f. limit use of University Technology Assets such as hardware and network for Personal Matters; and
g. acknowledge their access to sensitive data and complete all required training for the data to which they are authorized.

5. Users may not share or transfer university data, technology, or user credentials without prior authorization. Users must transfer possession or cease use when instructed by an appropriate manager.

6. Data and system users must uphold the confidentiality and privacy rights of individuals whose records they access; must adhere to controls based on Data Classification, including restrictions on access by Personal Technology Assets; must not disclose, share, or transmit data except as required by job duty or authorized in advance by the appropriate Data Steward and/or manager; and must accurately represent data, aggregations of data, or unit records when using, sharing, or transmitting data.

7. Users who access, utilize, and/or transport university data or technology away from university facilities must adhere to the *Secure Remote Access Guidelines (*http://tinyurl.com/z9naz7e*)* and applicable policies and procedures.

8. Individuals who use Personal Technology Assets to access or interface with university data, technology, or user credentials, are bound by this and other policies, related procedures, and guidelines.

9. Employees and organization units must use university-provided email accounts with a domain listed in Enterprise Data Standard 1.03, Email Domain Standard & Catalog (see http://tinyurl.com/z7k2p7k), and are prohibited from using personal or other external email accounts, for the conduct of university business. Employee and organization unit email accounts should not be auto-forwarded to personal or other external email accounts; this prohibits practices known as store-and-forward as well as forward-and-delete. This provision applies to student employees when receiving and sending university business-related email.

10. Managers are responsible for informing, orienting, and training employees, students, and other Constituents in the acceptable and responsible use of data, technology, and user credentials. They:
    a. must ensure that university data, technology and user credentials are appropriately authorized and issued based on job duties or other responsibility;
    b. must maintain accurate and current records of authorized access and technology issued to their personnel;
    c. must terminate or modify access in a timely manner for users who change job duties or responsibilities;

d. may restrict the use of Personal Technology Assets and/or may require exclusive use of University Technology Assets based on Data Classification, individual or organizational unit functions, job duty, and/or university procedures.
e. may impose additional restrictions on the use of University Technology Assets for Personal Matters, including use of Data and Information, hardware, and network.
f. must initiate and retain current and accurate documentation of *User Agreements* as well as external and internal data sharing agreements.

B. Definitions

1. **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).

2. **Consumable Software and Devices** are items purchased by the university which would cost more to track, reclaim, or redistribute than the original purchase price.

3. **Data and Information** (data and university data) are, individually or collectively, the known values, content, media (audio, visual, multimedia), information, intellectual property, official reports, and work product which the university or its organizational units collect, issue, produce, process, purchase, transmit, maintain and/or store regarding university Constituents, business processes, events, operations, performance, and services.

4. **Personal Matters** are individual or family concerns that are not related to the University, such as community activities and outside employment, including promotion, solicitation, services, or sales.

5. **Personal Technology Assets** are items that have been purchased, provided, or otherwise obtained by the User and are not considered University property. Examples include smart phones, tablets, personal computers, home network, and third-party services such as email and cloud storage.

6. **Principle of Least Privilege** (POLP) holds that every user of an asset should be authorized to, and should use, only the least set of privileges, rights, and permissions necessary to complete an assigned job or responsibility. In cases where assets, information systems, and services do not support strict controls, users are obligated to abide by POLP in their individual activities.

7. **University Technology Assets** are university owned hardware, devices, equipment, virtual desktop, software, information systems and services (whether on premises or not), databases and data stores, datacenters, learning management systems, network (including wired, wireless, Internet, and Virtual Private Network), audio, video, communications and telephony, which the university purchases, provides, or otherwise acquires.

8. **User Credentials** are accounts, email accounts, network username, other user names, identifiers and identity badges, digital identities (including those generated internally or under agreement with a third party or federated identity service), and the associated access rights, authorization, and services, which the university collects, requires, or issues in order to enable users to access data, information, communications, and/or technology, including for authentication.

9. **User** (or End User) refers to any person or system that accesses university assets including data and information systems.

II. Procedures

A. Procedures for All Campuses

1. Users must acknowledge they have received, read, and agree to follow this policy, related confidentiality and privacy provisions, standards, procedures, rules, and regulations pertinent to assets they are authorized to use. Users are required to complete a *User Agreement for Responsible Use and Confidentiality of Data, Technology, and User Credentials* (Appendix 1) prior to being authorized or granted access to data, technology, and user credentials.

2. Users are responsible for reporting known or suspected compromises of university data, technology, or user credentials to the University Information Security Office in a timely manner, in addition to other provisions of policy IT 3.00 (Information Security; see http://www.sc.edu/policies/ppm/it300.pdf) and the Information Security program, standards, and incident response process (see http://tinyurl.com/js463of).

3. 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 Memorandum of Agreement* (Appendix 2) prior to any sharing or transmission.

4. 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 Memorandum of Agreement* is executed prior to any sharing or transmission (Appendix 3).

5. 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.

6. User Credentials for non-human resources (sometimes referred to as Resource Accounts), such as those that enable transactions between information systems may be created and utilized only with: (1) appropriate manager authorization and designated ownership; (2) strict record-keeping of persons, purposes, and entities to whom the credentials are entrusted or applied; (3) scheduled and verified changes to the password; and (4) notice to and consent of Data Steward(s) of involved resources.

7. Users and managers must delete university data and information from Consumable Software and Devices prior to disposal or completely destroy Consumable Software and Devices if deletion cannot otherwise be ensured. Consumable Software and Devices shall not be tracked, reclaimed, or redistributed, unless otherwise directed by an appropriate manager.

III. Related Policies

ACAF 1.30	Access to Tenure and Promotion Application Files
ACAF 1.33	Intellectual Property Policy
ACAF 1.34	Use of Self-Authored Materials by Instructor
ACAF 1.39	Software
ACAF 3.03	Handling of Student Records
ACAF 7.03	Private Requests for University Data
BTRU 1.06	Audit & Advisory Services
BTRU 1.20	Dishonest Acts and Fraud
BUSF 4.12	University Identity Theft and Detection Program
BUSF 5.00	Property Accountability
BUSF 7.08	Cellular and Wireless Telephone and Devices
FINA 4.11	Credit/Debit Card Processing and Security
HR 1.22	Telecommuting
HR 1.39	Disciplinary Action and Termination for Cause
HR 1.69	Official Personnel Files and Records Release
IT 3.00	Information Security
LESA 3.06	Reporting Loss or Theft of University Property
RSCH 1.05	Data Access and Retention
STAF 1.02	Carolinian Creed
STAF 6.26	Student Code of Conduct
UNIV 1.51	Data and Information Governance

UNIV 2.00 Freedom of Information Policy

IV. Reason for Revision

Approval of this new policy is linked to repeal of UNIV 1.50 Data Access (revised August 6, 2010) and IT 1.06 Acceptable Use of Information Technology (revised September 21, 2012). This policy establishes a comprehensive policy addressing responsible use of university data assets, technology assets, and user credentials. Such provisions were previously held in two separate sections and policies: It retains and improves data access provisions of former UNIV 1.50; consolidates the information technology provisions of former IT 1.06; and adds new provisions for user credentials.

Certain policy provisions, when affirmed by individual user acknowledgement (Appendix 1) or other documentation (Appendix 2, 3, and 4), demonstrates compliance with State of South Carolina Division of Information Security "SCDIS-200 Information Security and Privacy Standards," issued September 18, 2015. As a state agency, USC is obligated to comply with these standards by July 2016.

UNIV 1.52: APPENDIX 1

TEMPLATE – USER AGREEMENT FOR RESPONSIBLE USE & CONFIDENTIALITY OF DATA, TECHNOLOGY, AND USER CREDENTIALS, VERSION 06/07/2016

Remove the header above and this section before presenting to User for signature.

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.*

Responsibility for Implementation
Data Stewards and managers of organizational units and personnel are responsible for ensuring this User Agreement is completed prior to any authorization or sharing of assets, including data, technology, and user credentials. The agreement shall be renewed annually by the user or more frequently if/when access and authorization changes are necessary. Data Stewards and/or managers may add content or supplemental requirements and documentation to this form, but should not remove content.

USER AGREEMENT FOR RESPONSIBLE USE AND CONFIDENTIALITY OF DATA, TECHNOLOGY, AND USER CREDENTIALS

Name of User: _____

Date: _____ Signature: _____

Office or Organization Unit: _____

Manager/Supervisor: _____ Signature: _____

I understand that by virtue of my employment or relationship with the University of South Carolina (USC), I may have access to University Technology Assets, including data, technology, user credentials, and other assets, which must be protected according to laws, regulations, policies, procedures and guidelines.

My signature above denotes that I have read and understand my responsibilities as outlined in the following USC policies and others available on the USC policy website http://www.sc.edu/policies/:

UNIV 1.51	Data and Information Governance
UNIV 1.52	Responsible Use of Data, Technology, and User Credentials
ACAF 3.03	Handling of Student Records
FINA 4.11	Credit/Debit Card Processing and Security
HR 1.22	Telecommuting
HR 1.69	Official Personnel Files and Records Release

IT 3.00	Information Security
LESA 3.06	Reporting Loss or Theft of University Property

I acknowledge that unauthorized access or disclosure, through my deliberate actions or negligence, of any data, information, technology, user credential, or other asset could subject me to criminal and civil penalties imposed by law. I further acknowledge that unauthorized disclosure or access may also constitute just cause for disciplinary action including termination of my employment on the first offense regardless of whether criminal or civil penalties are imposed. If I am ever in doubt about my responsibilities regarding USC data, technology, user credentials, or other assets, I will immediately consult my supervisor.

*****END APPENDIX 1*****

UNIV 1.52: APPENDIX 2

TEMPLATE – INTERNAL DATA AND INFORMATION SHARING MEMORANDUM OF AGREEMENT, VERSION 06/07/2016

Remove the header above and this section before providing to Recipient.

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 MOA is to specify the specific need and parameters of the sharing, including placing limits on the recipient for not further sharing data and information they receive.

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

The content below represents a model memorandum of agreement (MOA) 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 University Technology Services (UTS).

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, the Chief Information Security Officer, and Data Stewards of included data and information.

When requesting Student Data from Banner, requesting party must complete a formal request through the Data Access Permissions System (DAPS, https://www.sc.edu/daps/) and associated requirements.

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 MOA is executed prior to any sharing or transmission.

--- Memorandum content begins below this line---

INTERNAL DATA AND INFORMATION SHARING
MEMORANDUM OF AGREEMENT
UNIVERSITY OF SOUTH CAROLINA

This document constitutes a Memorandum of Agreement (hereinafter "MOA") between two or more organizational units of the University of South Carolina (hereinafter "USC"). The requested/sender party is _____ (hereinafter "Sender") and the requesting/receiving party is _____ (hereinafter "Recipient"). If any of the terms of this MOA conflict with any of the terms of other formal Agreements between the above named parties, the terms of this official agreement will control.

Description of Data and Information Sharing
The Recipient requests to be provided data and information from the Sender as follows:

Purpose
[detailed purpose/benefit/need/requirement of the Recipient for the requested information]

Data Elements Requested
[detailed list of data elements requested]

Source System
[name and describe the data store or system from which records are requested]

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]

Sharing Lifecycle
This agreement begins on [begin date] and terminates on [end date]. Note: the internal agreements must be reviewed and/or renewed annually at minimum.

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
If person records The Data Element included to ensure accurate identification of unique persons (known as a unique personal identifier) is: _____.

The data or information shared under this MOU ☐ includes or ☐ does not include Personally Identifying Information, 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

Ownership of Data and Information
Per policy UNIV 1.51 (Data and Information Governance) 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 Confidential Data
Recipient agrees to abide by limitations binding upon the USC 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://tinyurl.com/h43ojam).

Definition: Covered Data and Information (CDI) includes paper records, electronic images, data and other information records supplied by USC about its Constituents, operations, or business processes, as well as paper records, electronic images, data and other information records USC's Constituents provide directly to the Recipient, if any.

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.

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 or the University Information Security Office (UISO) 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.

The Sender's designated Point of Contact for this MOA 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 or Office]
[Published Phone Number]

***** END APPENDIX 2*****

UNIV 1.52: APPENDIX 3

TEMPLATE – EXTERNAL DATA AND INFORMATION SHARING MEMORANDUM OF AGREEMENT, VERSION 06/07/2016

Remove the header above and this section before providing to Receiving Entity.

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 template is a model memorandum of agreement (MOA) that USC organization units should complete with external organizations that receive and/or utilize university data or information, especially as required for mandatory reporting or other official purposes, and absent a formal contract or procurement. 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.

Responsibility for Implementation
University employees who are responsible for sharing or transmitting university data or information concerning university Constituents with PII with an external entity are responsible for ensuring this MOA 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
The Office of General Counsel and the Data Steward(s) of the particular university data or information will assist in explaining and/or negotiating terms of this Memorandum with the Receiving Entity.

--- Memorandum content begins below this line---

EXTERNAL DATA AND INFORMATION SHARING MEMORANDUM OF AGREEMENT

UNIVERSITY OF SOUTH CAROLINA

This document constitutes a Memorandum of Agreement (hereinafter "MOA") between the University of South Carolina or one of its organization unit (hereinafter "USC") and _____ (hereinafter "Receiving Entity"). If any of the terms of this MOA conflict with any of the terms of other formal Agreements or Contracts between the above named parties, the terms of the official agreement or contract will control.

Description of Data and Information Sharing
The University of South Carolina agrees to share data and information as follows:
[detailed description]

The data or information shared under this MOU ☐ includes or ☐ does not include Personally Identifying Information, 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

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: _____.

Agreement, Requirement, or Other Basis for Sharing
The sharing of data and information described above is required or otherwise deemed necessary due to the following:
[describe in detail the legislation, regulation, compliance obligation, or other requirement for sharing]

This requirement is in effect from [begin date] through and including [end date].

Ownership of Data and Information
Per policy UNIV 1.51 (Data and Information Governance) the University of South Carolina is the owner and legal custodian of its data and 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 Confidential Data
Receiving Entity agrees to abide by limitations binding upon USC related to the transmission, storage, access, and disclosure of Personally Identifiable Information (PII) 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://tinyurl.com/h43ojam).

Definition: Covered Data and Information (CDI) includes paper records, electronic images, data and other information records supplied by USC about its Constituents, operations, or business processes, as well as paper records, electronic images, data and other information records USC's Constituents provide directly to the Receiving Entity.

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 the Agreement 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 Agreement, 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: Upon termination, cancellation, expiration or other conclusion of the Agreement, Receiving Entity shall return all CDI to USC or, if return is not feasible, destroy any and all CDI. If the Receiving Entity destroys the information, the Receiving Entity shall provide USC with a certificate confirming the date of destruction of the data.

Remedies: If USC reasonably determines in good faith that Receiving Entity has materially breached any of its obligations under the Agreement, then USC, in its sole discretion, shall have the right to (1) require Receiving Entity to submit to a plan of monitoring and reporting and (2) provide Receiving Entity with a fifteen (15) day period to cure the breach. Before exercising any of these options, USC shall provide written notice to Receiving Entity describing the violation and the action it intends to take.

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 Agreement 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.

The USC designated Point of Contact for this MOA 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 or Office]
[Published Phone Number]

*****END APPENDIX 3*****

UNIV 1.52: APPENDIX 4

Template – Contract Addendum for External Data & Systems Service Providers
VERSION 06/07/2016

Remove the header above and this section before attaching to RFP, Contract, Purchase Order, etc.

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 agreement for USC organization units to include with any Request for Proposal (RFP) and procurement/purchasing for services, software, and systems that include university data or which support university or organization unit business processes. 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.

Responsibility for Implementation
University employees purchasing or otherwise acquiring services, systems, and software, including hosted services, which involve university data or business processes are responsible for ensuring this contract addendum is executed prior to payment for services (or renewal). This addendum shall not obstruct university contract approval or purchasing processes.

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, Purchasing Agent, 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 2.0.1 (June 2015; see http://tinyurl.com/jan8f8g), 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); see http://tinyurl.com/jan8f8g . 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: if procurement, purchasing, or other form of contract is <u>not</u> involved, this form should <u>not</u> be used; instead please refer to Template - External Data and Information Sharing Memorandum Of Agreement (Appendix 3).

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 Service Agreement will assist in explaining and/or negotiating terms of this Addendum with the Service Provider.

--- Addendum content begins below this line---

CONTRACT ADDENDUM FOR
EXTERNAL DATA & SYSTEMS SERVICE PROVIDERS

This document constitutes an Addendum to the Agreement 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 [*choose one:* the Solicitation; the RFP; the Contract, this Addendum] shall control.

Protection of Confidential Data
Service Provider agrees to abide by limitations binding upon the Institution 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://tinyurl.com/h43ojam).

Definition: Covered Data and Information (CDI) includes paper records, electronic images, data and other information records supplied by Institution about its Constituents, as well as paper records, electronic images, data and other information records the Institution's Constituents provide directly to the Service Provider, if any.

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: 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.

*****END APPENDIX 4*****