*User Agreement for Responsible Use and Confidentiality of Data, Technology, and User Credentials (Appendix 1)*

Version 08/30/2017, Chief Data Officer & Agency Privacy Liaison

**Authorization:**

* This template is known as Appendix 1 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.1 (Procedures for All Campuses)**

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.

*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*. Once authorized, this agreement is generally sufficient to enable the named user to request or receive exchanges of data, or system access, for the conduct of their routine work responsibilities. (Note: for more substantial internal data exchanges, including data integrations and seed data for information systems, please use Appendix 2.)

*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.

*Remove all content above before presenting to User for signature*

**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.

The University of South Carolina is committed to protecting student privacy for students enrolled in all courses regardless of the mode of instruction (classroom, blended, online). All of the University policies regarding students’ privacy and information security apply to distributed learning and traditional on-campus courses. 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. In the event access is determined to be contrary to university policy or applicable law, appropriate measures will be taken, including referral to student, employee, or faculty disciplinary processes. . If I am ever in doubt about my responsibilities regarding USC data, technology, user credentials, or other assets, I will immediately consult [fill in appropriate contact such as supervisor/office/department].