NUMBER: UNIV 1.52

SECTION: University Administration

SUBJECT: Responsible Use of Data, Technology, and User Credentials

DATE: June 30, 2016

REVISED: May 5, 2017

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's statutory 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 data, including University Data (see UNIV 1.51), 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 they initiate or conduct 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 must 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.

11. The Vice President for Information Technology and Chief Information Officer is responsible for administration, coordination, and clarification of this policy.

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) 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. See also University Data (UNIV 1.51).

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 Business** describes processes, transactions, communications, and records produced or received by a USC employee or a party acting on behalf of the university, regarding actions, operations, services, and Constituents of the university or its units, as well as official university reports, requests, policies, and procedures; any matter subject to Freedom of Information Act (see UNIV 2.00) is considered University Business. Such data may include, but is not limited to, human resources, student records, alumni/development, and other administrative information; data classified as Restricted, Confidential, or Internal Use is most often included (see UNIV 1.51).

   The term University Business excludes teaching and learning activities, as well as academic research data, personal property, items that are public record, and intellectual property (see ACAF 1.33).

8. **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.

9. **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.

10. **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 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 Certification* 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

Revised to formally establish and define the term University Business and to clarify wording of I.A.4.d.

Appendixes are now hosted on the website of the Chief Data Officer, and linked from within the policy. Based on comments received following initial approval, Appendix 1 was revised to remove specific consequences and instead refer to existing procedures for students, faculty, and staff and to clarify its intended use. Appendix 2 was revised to clarify and limit intended use of the appendix for substantial internal data exchanges, such as for system integrations. Appendix 3 was revised to clarify use and nature of certification by external entity per request of General Counsel.

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.