ADMINISTRATIVE DIVISION UNIV University Administration		POLICY NUMBER UNIV 1.52
POLICY TITLE Responsible Use of Data, Technology, and User Credentials		
SCOPE OF POLICY USC System	DATE OF REVISION Month XX, XXXX	
RESPONSIBLE OFFICER Vice President of Information Technology and Chief Information Officer	ADMINISTRATIVE OFFICE Division of Information Technology	

PURPOSE

All individuals and organizational units accessing or using university data, technology, and user credentials are required to adhere to all applicable state and federal laws, statutes, and regulations, as well as university policies, standards, and procedures. Access and use must be authorized based on job responsibilities or a demonstrated need, ensuring that the availability, confidentiality, integrity, privacy, and security of university assets are not compromised.

To fulfill its mission, the University of South Carolina (USC) is committed to safeguarding the confidentiality, integrity, and availability of its data, technology, and user credentials. USC upholds responsible use of these resources, strictly prohibiting unauthorized access or personal use unrelated to university purposes. Any misuse may lead to investigation and potential disciplinary actions according to human resources and student conduct policies.

DEFINITIONS AND ACRONYMS

Artificial Intelligence (AI): technology that increasingly enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy. Applications and devices equipped with AI often include, but are not limited to, the following capabilities: can see and identify objects; can understand and respond to human language; can learn from new information and experience; can make detailed recommendations to users; can sometimes act independently, potentially replacing or reducing the need for human intervention.

Constituents: 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, service providers and volunteers).

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

Data and Information: refers to the individual or collective values, content, media (including audio, visual, and multimedia), intellectual property, official reports, and work products that the university and its units collect, process, transmit, store, or maintain. This encompasses all details about university constituents, business processes, events, operations, and

services. In the context of Artificial Intelligence, data also includes inputs used to train AI models and algorithms, which transform raw data into meaningful insights, predictions, and decision-making tools. These AI-driven processes enable the university to enhance its operations while ensuring the responsible and ethical handling of data in compliance with applicable laws and regulations (see policy UNIV 1.51 Data and Information Governance).

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

Personal Technology Assets: refer to devices, software, and services that are owned, purchased, or acquired by the User and are not classified as university property. These include smartphones, tablets, personal computers, home networks, third-party services such as email and cloud storage, and Artificial Intelligence (AI) tools or platforms that the User employs independently. AI tools, such as generative AI applications, voice assistants, or personal AI models, are considered part of Personal Technology Assets when used outside of university-authorized resources or environments.

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.

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 policy UNIV 2.00 Freedom of Information Policy) 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 policy UNIV 1.51 Data and Information Governance). 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 policy ACAF 1.33 Intellectual Property Policy).

University Technology Assets: include all university-owned hardware, devices, equipment, virtual desktops, software, information systems and services (whether on-premises or cloud-based), databases, data stores, data centers, learning management systems, and network infrastructure (wired, wireless, Internet, and Virtual Private Network). This also encompasses audio, video, communications, and telephony systems that the university purchases, provides, or acquires. Additionally, these assets include any Artificial Intelligence (AI) technologies and services used to support university functions, enhancing data processing, decision-making, research, and operational efficiency.

User Credentials: 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.

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

POLICY STATEMENT

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

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

C. The university requires the Principle of Least Privilege (POLP) by limiting access to its assets based on job duties or other demonstrated need, while recognizing that privilege and access are often necessary to provide value to University Constituents, achieve operational excellence, and gain competitive advantage.

D. All users have a direct personal responsibility for the appropriate use of data, including University Data (see policy UNIV 1.51 Data and Information Governance), technology, and user credentials; all users must comply with this policy and related standards and procedures, and must:

1. protect and properly use these assets regardless of their physical location;

2. adhere to applicable state and federal laws, statutes, and regulations;

3. abide by USC policies, procedures, guidelines, and privacy and security protections and controls;

4. accept responsibility for all activity they initiate or conduct through the use of their user credentials;

5. refrain from accessing or using University Data and Information for Personal Matters;

6. limit use of University Technology Assets such as hardware and network for Personal Matters; and

7. acknowledge their access to sensitive data and complete all required training for the data to which they are authorized.

8. AI technology must not be used to create content that is inappropriate, discriminatory, deceptive, or otherwise harmful to others or the University. All AI-generated content must be carefully reviewed for accuracy, appropriateness, and bias before relying on it for work purposes.

E. 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.

F. 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.

G. Users who access, utilize, and/or transport university data or technology away from university facilities must adhere to the Secure Remote Access Guidelines and applicable policies and procedures.

H. 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.

I. Employees and organization units must use university-provided email accounts with a domain listed in Enterprise Data Standard 1.03, Email Domain Standard & Catalog 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.

J. 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:

1. must ensure that university data, technology and user credentials are appropriately authorized and issued based on job duties or other responsibility;

2. must maintain accurate and current records of authorized access and technology issued to their personnel;

3. must terminate or modify access in a timely manner for users who change job duties or responsibilities;

4. 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.

5. may impose additional restrictions on the use of University Technology Assets for Personal Matters, including use of Data and Information, hardware, and network.

6. must initiate and retain current and accurate documentation of User Agreements (see Appendix 1) as well as Data Sharing Agreements with internal and external entities (see Procedure below).

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

PROCEDURES

The accompanying procedure provides additional details on the administration and management of this policy. The procedure can be found here: Information Technology Policies - Division of Information Technology | University of South Carolina

RELATED UNIVERSITY, STATE AND FEDERAL 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 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
FINA 2.30 Wireless Communication Stipends
FINA 8.11 Credit/Debit Card Processing and Security
FINA 8.12 University Identity Theft and Detection Program
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
RSCH 1.05 Data Access and Retention
STAF 6.26 Student Code of Conduct
UNIV 1.51 Data and Information Governance
UNIV 2.00 Freedom of Information Policy

HISTORY OF REVISIONS

DATE OF REVISION	REASON FOR REVISION
June 30, 2016	New policy approval
May 5, 2017	Substantive revision
April 9, 2018	Reformatted policy to the new template.
August 4, 2024	Remove links to specific appendixes (no longer self-service templates due to confusion and misuse), and to align with changes to policy UNIV 1.51. Revised purpose for conciseness and clarity. Incorporated Artificial Intelligence usage and responsibility in several definitions. Confirmed all linked URLs.

Month XX, XXXX This will be the approval date	Changing the word “promotes” to “requires” to prepare for configuration standardization across university devices. This means systems and access settings will follow consistent, centrally managed standards rather than individual or departmental preferences. Using “requires” clarifies that following the Principle of Least Privilege—giving people only the access they need to do their jobs—is not optional. This change helps protect university data and ensures consistent security practices across all areas.

APPENDICES

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