PROCEDURE NUMBER:	UNIV 1.52 Procedure
SECTION:	Division of Information Technology
SUBJECT:	Responsible Use of Data, Technology, and User Credentials
DATE:	June 30, 2016
REVISION:	April 27, 2026
Procedure for:	USC System
Authorized by:	Vice President for Information Technology and Chief Information Officer
Issued by:	Division of Information Technology – VPCIO Office

Procedure

The Division of Information Technology, VPCIO Office, will ensure compliance with UNIV 1.52. This procedure is applicable to campuses, units, departments, centers, and administrators at the University who are involved with the USC System. The purpose of this procedure is to supplement the associated policy by providing additional detail regarding Responsible Use of Data, Technology, and User Credentials.

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* 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 and the Information Security program, standards, and incident response process.

3. University organizational units that require exchange, transmission, or other sharing of data and information, whether with other org units in the USC System or with an external entity, must establish and adhere to a Data Sharing Agreement prior to any sharing or transmission. Units should initiate a Data Governance Data Sharing Agreement Assistance request through Division of Information Technology Service portal.

4. University employees and units seeking to purchase or acquire data and/or technology, systems, software and/or services that use or produce University Data are responsible for adhering to all purchasing laws and procedures. This includes adherence to policy IT 1.00 Information Technology Procurement and related procedures.

   Units should initiate a Data Governance Data Sharing Agreement Assistance request through Division of Information Technology Service portal at the same time that they initiate inquiries or activities with the Purchasing Department. Generally, provisions for a *Data Sharing Agreement(s)* should be established through solicitations (RFP, RFQ, Sole Source requests, or renewals) prior to finalizing awards, contracts, and/or initiating or renewing contracts and services. Data Sharing Agreements are needed when acquiring services from a third party for which data is not the focus, but which involves University Data. For systems acquired via RFP after January 2023, the contract's Special Terms and Conditions specifies the data handling requirements. For non-RFP acquisitions or RFPs before January 2023 a Data Sharing External Signature Agreement must also be established and signed prior to any sharing or transmission. Since this agreement is between USC and an external entity, the Data Sharing External Signature Agreement must be signed by the Secretary of the Board of Trustees, or another authorized signatory as specified in policy BTRU 1.04 Authority to Sign Contracts.

B. Instructions for Obtaining an Agreement with an External Entity:

- Send the document to the vendor for signature
- Once returned, prepare a package for General Counsel, including:
  - Cover memo
  - Contract Approval Form
  - Signed Data Sharing External Signature Agreement (Please note – The contract approval form has specific instructions for submission to General Counsel)

- 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.

- 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.

C. Standard User Accounts and Local Administrative Privileges

1. **Purpose**
   In accordance with the Principle of Least Privilege (POLP) articulated in UNIV 1.52, all standard user accounts authorized to access University Technology Assets must be limited to the minimum privileges necessary to perform assigned duties. Standard user accounts **must not be utilized as local administrator accounts** on University-owned devices, except through an approved escalation process as described below. Granting administrative privileges to standard user accounts increases security risk and may compromise the confidentiality, integrity, or availability of University data and systems.

2. **Definitions**
   a. *Standard User Account* -A user account provisioned for an individual for general computing activities and access consistent with job responsibilities.
   b. *Local Administrator Privileges* -Permissions on a device that allows full control over system settings, software installation, configuration changes, security settings, and installation of services or drivers.

3. **General Requirement**
   a. Standard user accounts must not be members of the local Administrators group on University-owned laptops, desktops, tablets, or other endpoint devices as a default configuration.
   b. Local administrator privileges shall only be issued when there is a documented business justification, the privilege is essential for specific job functions that cannot be performed without administrator rights, or the access is approved following the procedures below.

4. **Procedure for Requesting Local Administrative Access**
   a. A request for local administrative privileges must be submitted to the relevant departmental IT support unit or Division of Information Technology (DoIT) service desk. The request must include:
   i. Justification demonstrating that the duties cannot be completed within a standard user context and that elevated privileges are necessary;
   ii. Duration for which the elevated access is required; and
   iii. Manager or supervisor approval affirming the business need.
   b. The IT support unit or DoIT shall evaluate the request for appropriateness, alignment with security standards, and alternative controls that could satisfy the requirement without elevating privileges (e.g., use of managed software deployment, role-based management tools, or temporary privilege elevation).
   c. Approved local administrative privileges shall be:
   i. Documented and retained in accordance with University record retention practices;
   ii. Assigned to a separate administrative account when supported by system capabilities; and
   iii. Limited in scope and time as necessary to perform the approved function.

5. **Monitoring, Review, and Revocation**

   a. Local administrative privileges granted under this section must be reviewed at least annually by the responsible IT unit to determine whether the privileges remain necessary.

   b. Privileges shall be revoked immediately when no longer required for job functions, when access is misused, or upon termination of employment or contract.

   c. Periodic audits shall be conducted to ensure compliance with this procedure and the broader requirements of UNIV 1.52.

6. **Security and Reporting**

   Users granted local administrative privileges must complete any required security awareness training and are responsible for reporting any suspected compromise of credentials, changes, or unauthorized activity in accordance with reporting obligations under Section A of this Procedure and policy IT 3.00.

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.
January 12, 2026	Procedure is now separate from policy
April 27, 2026	Add Standard User Accounts and Local Administrative Privileges (Section C)