1. Access Management Policy

Issued: May 3, 2019
Last Revised: October 24, 2022
Last Reviewed: October 24, 2022

2. Policy Purpose

This Access Management Policy documents university requirements of user access throughout the access management lifecycle from the identification of a user to the granting, modifying, or revoking of a user’s access privileges.

3. Scope and Application

This policy applies to all:

- University faculty members (including part-time and visiting faculty)
- Staff and other employees (such as postdoctoral scholars, postdoctoral fellows, and student workers)
- iVIP (guests with electronic access), as well as any other users of the network infrastructure, including independent contractors or others (e.g., temporary agency employees) who may be given access on a temporary basis to university systems
- Third parties, including vendors, affiliates, consultants, and contractors

4. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Governance, Risk, Compliance (IS GRC)</td>
<td>A combination of three approaches that organizations use to demonstrate compliance with international standards, global rules, laws, and state regulations. Governance, risk management, compliance (GRC) is often implemented by companies that are growing globally to maintain consistent policies, processes, and procedures across all parts of the organization</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>Least Privilege Access</td>
<td>A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions</td>
</tr>
<tr>
<td>Privileged Access</td>
<td>Privileged Access: This consists of the following;</td>
</tr>
<tr>
<td></td>
<td>• Administrative access to systems or data (e.g., server or database administrators)</td>
</tr>
<tr>
<td></td>
<td>• Access to systems and resources beyond standard user levels and permissions</td>
</tr>
<tr>
<td></td>
<td>• Ability to modify security settings, create users, and grant access</td>
</tr>
<tr>
<td></td>
<td>• Ability to bypass or circumvent security controls</td>
</tr>
</tbody>
</table>
For more definitions and terms: USC Information Security Policies Terms and Glossary

5. Policy Details

Objective

The objective of this policy is to ensure that user access is managed appropriately throughout the access management lifecycle for USC assets and information systems.

Policy Requirements

5.1 System Owners are responsible for monitoring and controlling all user access to associated USC data, assets and information systems.
5.2 System Owners will document, implement and maintain formal user registration and revocation processes for access to USC data, assets and information systems.
5.3 System Owners will prevent the reuse of identifiers that uniquely identify each individual user and will only assign an individual one identifier (no more than one University ID and one personal USC NetID).
5.4 System Owners will provision accounts to users in a manner adhering to the Least Privilege Access concepts, which calls for limiting access to only the information and resources necessary for a task or role.
5.5 Prior to granting access, the System Owner will verify that the access requested is appropriate for the user's role and responsibilities.
5.6 Prior to granting access, the System Owner or an authorized delegate when appropriate, will approve and document access requests.
5.7 System Owners will grant Privileged Access exclusively when such access is required.
5.8 When granting Privileged Access, System Owners will require approval by appropriate organizational personnel commensurate to the level of risk associated with that access.
5.9 Accounts with Privileged Access should not be used for non-privileged activities, including internet use, email communications, and other activities that could be otherwise accomplished with a non-privileged account.
5.10 Accounts with Privileged Access should be managed by a system approved by Office of the CISO that stores credentials and provides a method to audit access.
5.11 System Owners will require appropriate authentication prior to user's access to USC data, assets, and information systems.
5.12 System Owners who provide authentication services (e.g., Active Directory, sign-on, multifactor authentication) will document and register the system with OCISO.
5.13 Multifactor authentication should be used for Privileged Access functions (where applicable if multifactor authentication is supported by the system) consistent with job level, job duties, and the classification of data as described within the Data Protection policy.
5.14 Consistent with the Least Privilege Access concepts, service accounts and shared maintenance accounts will be treated as Privileged Access accounts, documented in an inventory with authorized approvals and for stated purposes only.
5.15 All manufacturer default accounts will be deleted, disabled, and/or renamed. If unable to delete, disable, and/or rename the default accounts, passwords should be changed.
5.16 System Owners will provision critical system access to separate individuals (e.g., segregation of duties to prevent conflicting responsibilities to the same person that may result in compromised security, fraud, or error).

5.17 Access privileges will be reviewed periodically using a formal process consistent with job level, job duties, and the classification of data as described within the Data Protection policy.

5.18 System Owners will modify or disable access upon notification of a transfer, termination, or other significant change to a user's employment status or role.

5.19 System Owner will disable user accounts within three business days upon notification when user's employment terminates.

5.20 System Owners will implement immutable logging on systems to capture privileged security events including user account creation, modification, password resets, password changes, and access removal/deletion.

5.21 System Owners will implement immutable logging on authentication services to capture logon events.

5.22 Individuals will not share with or transfer their passphrase to others that allow them to gain unauthorized access to USC information technology resources.

5.23 Validate that all privileged users are using named accounts and not using shared accounts (e.g., bobtaylor vs root).

5.24 Review all privileged accounts and confirm that each meets the USC passphrase policy and has Multi-factor Authentication (MFA)

5.25 Complete access review to remove all terminated user accounts, who longer need access, from environments.

5.26 Implement Multifactor Authentication on all USC related email accounts.

6. Procedures
None

7. Forms
None

8. Responsibilities
All Faculty and Staff are required to comply with this policy.

9. Related Information

Compliance Measurement
The Office of the CISO and the Office of Audit Services will collectively monitor compliance with this policy, USC’s information security policies and standards, and applicable federal and state laws and regulations using various methods, including but not limited to periodic policy attestations. Compliance with information security policies will be monitored regularly in conjunction with USC’s monitoring of its information security program. Audit Services will conduct periodic internal audits to ensure compliance.

Exceptions
Any exceptions to the policy will be submitted and approved in accordance with the Information Risk Committee decision criteria by the OCISO Governance, Risk Management, and Compliance. Exceptions will be requested via email to the OCISO Governance, Risk Management, and Compliance team at infosecgrc@usc.edu.
Non-Compliance
Violation of this policy may lead to this being classified as a serious misconduct, which is grounds for discipline in accordance with the Faculty Handbook, staff employment policies, and SCampus, as appropriate. Any disciplinary action under this policy will consider the severity of the offense and the individual’s intent and could include termination of access to the USC network, USC systems and/or applications, as well as employment actions up to and including termination, and student disciplinary actions up to and including expulsion.

10. Contacts
Please direct any questions regarding this policy to:

<table>
<thead>
<tr>
<th>OFFICE</th>
<th>PHONE</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Chief Information Security Officer</td>
<td></td>
<td><a href="mailto:trojansecure@usc.edu">trojansecure@usc.edu</a></td>
</tr>
</tbody>
</table>