USC University of Southern California

1. Passphrase Policy

Issued: September 28, 2018

Last Revised: October 24, 2022
Last Reviewed: March 29, 2023

2. Policy Purpose

The purpose of this Policy is to outline the acceptable use of passphrases at the University of Southern California (USC).

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

Term	Definition
System Owner	The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The System Owner is a key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented

For more definitions and terms: USC Information Security Policies Terms and Glossary

5. Policy Details

Objective

Eligible individuals are provided access to support their studies, instruction, research, duties as employees, official business within USC, and other USC sanctioned activities. Individuals will not share with or transfer their passphrase to others that allow them to gain access to USC information technology resources.

Policy Requirements

Each information system that provides access to any USC data will adhere to the passphrase policy and will meet the following requirements:

5.1 The system will have a defined System Owner responsible for the implementation of the requirements of this policy.
5.2 The allocation and modification of passphrases will be controlled and securely configured through a formal process in accordance with Identity and Access Management (IAM) standards.
5.3 USC user passphrases will adhere to the applicable Passphrase Standard, and when integrating with Single Sign-On (SSO) capabilities.
5.4 Passphrase policy and standards will be monitored and reviewed periodically.
5.5 Utilize USC recommended password manager for USC-Owned Technology Resources, critical business operations.

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 the Student Handbook, 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:

OFFICE	PHONE	EMAIL
Office of the Chief Information Security Officer		trojansecure@usc.edu