USC University of Southern California

Access Management Standard

Document ID Reference: ST21

Issue Date: 4/7/2023 **Effective Date:** 4/7/2024

DOCUMENT CONTROL

DOCUMENT NAME: Access Management Standard
DOCUMENT ID REFERENCE: ST21

AUTHORIZATION:

Prepared By	**Reviewed By**	**Approved By**
IS GRC Staff	Sandy Taylor	Gus Anagnos
	Sr. Director Security Strategy & Governance	CISO
Date: 2/28/2023	Date: 4/6/2023	Date: 4/6/2023

VERSION HISTORY:

Version	Issue Date	Effective Date	Prepared By	Authorized By	Description
1.0	4/7/2023	4/7/2024	Information Security Governance, Risk & Compliance	Gus Anagnos	Original version

1.0 Introduction

1.1 Purpose

The Access Management Standard establishes the information security monitoring, management, and control of user access to USC data, assets, and information systems at schools and units across USC.

1.2 Scope

This Standard applies to USC System Owners who maintain or operate USC information systems.

1.3 Objective

This Standard is designed to communicate the baseline security requirements for user access to USC information systems considered High Value Assets (HVAs) or assets with Confidential data.

2.0 Standard Requirements

2.1 General User Access Requirements

2.1.1 System Owners will establish a process to ascertain accurate information (i.e., ID, student enrollment, employment status) about a user (i.e., student, staff, affiliate) to administer the user's access from official USC systems of records.

2.1.1.1 Student user information will be ascertained from the Student Information System (SIS) system of record.

2.1.2 System Owners will document and implement a process for assessing, creating, changing, and/or disabling access in accordance with their status and relationship with USC.

2.2 Student User Access Requirements

The following requirements listed below apply to USC students. Individuals who simultaneously hold student and USC employee, iVIP, or student worker status should maintain access in accordance with their status and relationship with USC that is relevant at a given time.

2.2.1 System Owners will implement a process to disable access for students who have a conferred degree (i.e., graduated) approximately one (1) year after the end of the student's last enrolled semester, or approximately one (1) year after the end of the semester during which the student's degree was awarded, or approximately one (1) year beyond the end of the semester in which the degree was conferred, whichever is more recent.

2.2.2 System Owners will implement a process to disable a student's access within thirty (30) business days after a student is expelled from USC or deceased, ideally three (3) business days.

2.2.3 System Owners will implement a process to disable access for students who leave the university for any reason other than those described above, approximately two (2) years after the end of the student's last enrolled semester.

3.0 Standard Compliance

3.1 Compliance Measurement

The Office of the CISO and the Office of Audit Services will collectively monitor compliance with this standard, 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 and standard attestations. Compliance with information security policies and standards 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

3.2 Exceptions

Any exceptions to the standard will be submitted, assessed, and approved or denied in accordance with the Information Risk Committee by the OCISO Governance, Risk

Management, and Compliance team. Exceptions will be requested via email to the OCISO Governance, Risk Management, and Compliance team at **infosecgrc@usc.edu**.

3.3 Non-Compliance

Violation of this standard may be classified as serious misconduct, which is grounds for discipline in accordance with the Faculty Handbook, staff employment policies, and SCampus, as appropriate. Any disciplinary decision under this standard 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.

4.0 Governing Policies, Related Standards, and Processes

- Access Management Policy
- Network Security Policy
- Passphrase Policy
- USC Information Policies – Terms and Glossary
- SCampus Part F - Other University Policies

5.0 Definitions and Terms

- **Information Security (InfoSec)**: Information security - protecting against the unauthorized use of information, especially electronic data, or the measures taken to achieve this
- **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, visit the USC Information Security Policies Terms and Glossary

6.0 Standard Revision

All revisions to this Standard will be made with the approval of the OCISO Governance, Risk Management, and Compliance team, Information Risk Committee and USC General Counsel.

7.0 Standard Acknowledgement

Periodically, all authorized users will be required to read and acknowledge understanding this standard.