## 1. Security Awareness Training Policy

Issued: July 18, 2019
Last Revised: December 1, 2020
Last Reviewed: November 11, 2022

## 2. Policy Purpose

This Security Awareness Training Policy establishes university requirements for information security awareness training and sets minimum expectations for completing such training.

## 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)

## 4. Definitions

| Term | Definition |
|---|---|
| AUP | Acceptable Use Policy |
| Information Security Governance, Risk, Compliance (IS GRC) | 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 |
| ITS | Information Technology Services |
| OCISO | Office of the Chief Information Security Officer |

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

## 5. Policy Details

### Objective

Everyone covered by this policy is responsible for protecting the University of Southern California's (USC) information assets. USC's information security awareness training program is designed to communicate minimum requirements for user behavior in protecting USC information assets.

### Policy Requirements

5.1 Information security awareness training will provide users with education on relevant information security risks and explain the importance of information security at USC.

5.2 Information security awareness training will be provided upon new hire on-boarding and at least annually for all covered individuals within scope, including USC employees, faculty, and student workers.

5.3 Periodic targeted and/or role-based information security awareness training should be provided on an as-needed basis as determined by the Chief Information Security Officer (CISO) or by the leadership within a school or unit.

5.4 Information security awareness training will be completed annually.

5.5 Each manager is responsible for tracking completion of information security awareness training for the respective direct reports. Evidence of compliance may be requested by the Office of the CISO.

5.6 Covered individuals will acknowledge relevant information security policies at least annually.

## 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 |