1. Acceptable Use Policy

Issued: May 3, 2019
Last Revised: December 1, 2020
Last Reviewed: November 11, 2022

2. Policy Purpose

This Acceptable Use Policy (AUP) describes university expectations for the appropriate use of University of Southern California (USC) Owned Technology Resources including software, internet services, email services, computer, and electronic devices.

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
- Students

4. Definitions

Term	Definition
AUP	Acceptable Use Policy
Covered Individuals	People or entities specified by the scope of a policy
Internet Services	Access to internet provided by USC
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
Junk Email	Unwanted or unsolicited email, typically in the form of advertising or promotional material
Local Technology Support	Information technology support dedicated within a local school or unit
Network Services	A capability that facilitates a network operation, such as WIFI, Voice over IP (VOIP), Local Area Networks, etc.
OCISO	Office of the Chief Information Security Officer
Personal Devices	Refers to devices, such as a laptop, tablet or smartphone owned by an individual, and not owned, reimbursed or paid for by USC

SVP	Senior Vice President
USC-Distributed	Infrastructure, licensing or devices provided by USC
USC-Owned	Asset owned, reimbursed or paid for by University of Southern California
USC-Owned Technology Resources	USC network-based communication services and file repositories (including but not limited to, USC networks, USC email accounts, USC instant message, and USC cloud-based repositories); USCissued computers and electronic devices (including but not limited to, desktops, laptops, servers, mobile phones, tablets, PDAs, and pagers) that are purchased or leased using university funds; and USC purchased, licensed, or developed software

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

5. Policy Details

Objective

The objective of this policy is to document the appropriate use of USC-Owned Technology Resources (including, but not limited to, communication sources, software, internet services, email services, file repositories, instant messaging, USC related cloud services computer, electronic and devices), and activities performed using USC networks.

Access to USC-Owned Technology Resources is provided to support faculty and staff in their day-to-day university related tasks and to provide students with needed resources for their educational pursuits. Although limited or incidental personal use may be permitted (as outlined in SCampus, the faculty handbook, and staff employment policies), USC has established proper use of these resources.

USC-Owned Technology Resources are the property of USC. There is no expectation of privacy when using USC-Owned Technology Resources. USC may monitor and inspect files and communications on USC-Owned Technology Resources at any time.

Policy Requirements

Acceptable use of USC-Owned Technology Resources. USC reserves the right to monitor, inspect, retrieve, and review all technology resources for security purposes, including but not limited to identifying, investigating, and reporting any violations against this or other USC policy. Covered individuals will:

5.1 Use USC-Owned Technology Resources for legitimate USC business purposes**.** Covered Individuals are advised there is no right to privacy in any USC-Owned Technology Resources.

5.2 Be responsible for their use of any USC-Owned Technology Resource; including but not limited to computers, laptops, removable media, electronic files, routers, servers, and all USC-Distributed or third-party supplied software, and of any appropriate or authorized use carried out under their delegation.

5.3 Not attempt to break into or adversely affect the performance, management, or security of internal or external USC-Owned Technology Resources, such as by:

5.3.1. Consuming an excessive amount of system resources that adversely affects other users (e.g., crypto mining).
5.3.2. Blocking administration and/or management of the network infrastructure.
5.3.3. Illegal activities in violation of civil or criminal law, including but not limited to hacking, theft, and dark web transactions.

5.4 Not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to damage, or otherwise hinder the performance of any USC technology resource or network system. Such software may be called a virus, worm, or a Trojan horse.

5.5 Not interfere with the normal functioning of USC-Owned Technology Resources, adversely affect the ability of others to use these technology resources, or harm others.

5.6 Not tamper with or disable security technical mechanisms. Examples of such security technical mechanisms are malicious program detection or remediation software.

5.7 Not access, without authorization, USC-Owned Technology Resources, including but not limited to, files, directories, shared drives, or accounts. If a vulnerability or open directory is discovered, notify OCISO (security@usc.edu) as soon as possible.

5.8 Not test or attempt to compromise technology resource security measures unless specifically approved in advance and in writing by the Office of the Chief Information Security Officer (OCISO). Likewise, shortcuts bypassing system's security measures, as well as pranks and practical jokes involving the compromise of security measures, are prohibited. If a vulnerability or software bug is discovered, notify OCISO (security@usc.edu) as soon as possible.

5.9 Not use any USC-Owned Technology Resources to defame, libel, abuse, or portray in a false light, USC or any of its students, partners, affiliates, or workforce as defined in USC handbooks and policies. Nothing in this policy is designed or intended to interfere with, restrain, or prevent employee communications regarding wages, hours, or other terms and conditions of employment.

5.10 Not use USC-Owned Technology Resources to promote or maintain business for solely personal gain or compose or forward chain letters or offensive jokes.

5.11 Promptly return all USC-Owned Technology Resources upon request or during separation from the university to the Asset Owner. USC-issued devices must be returned on or before the last day of employment.

5.12 If a USC-Owned Technology Resource asset is lost or stolen, Covered Individuals will:

5.12.1. If possible or applicable, file a police report. Contact the Asset Owner and provide the police report number, device brand, model, and indicate that the device is owned by USC.
5.12.2. Contact Local Technology Support, fill out relevant forms, and follow applicable escalation procedures.
5.12.3. If you suspect that confidential information, about the Data Protection Policy, was on the lost or stolen device, notify OCISO (security@usc.edu) of the lost or stolen device, and provide the police report number associated with the incident.

Acceptable use of software for personal, professional, and academic development as it relates to USC-Owned Technology Resources. Covered individuals will:

5.13 Not install or use unlicensed software, such as stolen or cracked software, on USC-Owned Technology Resources.

5.14 Not share USC purchased licenses with unapproved individuals.

5.15 Not use software or hardware tools intended to defeat software copy protection, discover other users' passwords without consent, identify security vulnerabilities with malicious intent, decrypt encrypted files without appropriate authorization, or to compromise information security on USC-Owned technology resources, or non-USC-Owned Technology Resources connecting to the USC network unless authorized by OCISO.

Acceptable use of USC email services. Covered Individuals will:

5.16 Retain and manage email in accordance with USC's records retention schedule and its records retention requirements, as referenced in the Data Protection Policy.
5.17 Not send USC Confidential or Internal Use Only information to personal email accounts or automatically forward USC emails to personal accounts.
5.18 Not send Confidential Information, as defined in the Data Protection Policy, through email in an unencrypted format.
5.19 Not send inappropriate information or Junk Email via email to other USC Covered Individuals, including but not limited to fraudulent, malicious, phishing, and/or spam emails.

Acceptable use of All Devices, including Personal Devices. Covered Individuals may be permitted to bring Personal Devices (e.g., smart phones) into USC locations for personal use (e.g., personal education, personal calls). Covered Individuals will:

5.20 Cooperate with legal investigations by providing prompt access to any devices in accordance with the law.

Acceptable use of USC-Owned Network Services. Covered Individuals will:

5.21 Not use Network Services to send or distribute messages in violation of law or USC policies or in a manner that otherwise creates a hostile work environment.
5.22 Not use Network Services to circulate illegal materials (e.g., child pornography) nor infringe on copyright protections in violation of civil or criminal law.
5.23 Expect that access and use of USC-Owned Technology Resources, including but not limited to; Internet Services, Email, Devices, etc. are logged and monitored.

6. Procedures

None

7. Forms

None

8. Responsibilities

All Faculty, Staff and Students 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:

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