1. Acceptable Use Policy

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

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 Califo
USC-Owned Technology Resources	[illegible]

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