1. Asset Management Policy

Issued: May 3, 2019
Last Revised: October 24, 2022
Last Reviewed: October 24, 2022

2. Policy Purpose

This Asset Management Policy establishes security requirements for effective management, control and protection of the hardware assets (including leased assets) within an organization, throughout all stages of their lifecycle at the university, for asset management related to information assets and/or systems.

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
Asset Custodian	All IT assets are wholly owned by USC, but the Asset Custodian is the person primarily responsible for the asset. This is traditionally the individual who procured and/or provisioned the asset, or the person for which the asset was procured for
Asset User	The person in possession of the asset or executing the function of the asset. This person may have been provisioned an asset by the Asset Custodian, who is ultimately responsible for the asset. All IT assets are wholly owned 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
USC-Owned	Asset owned, reimbursed or paid for by University of Southern California

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

5. Policy Details

Objective

The objective of this policy is to have designated Asset Custodian appropriately procure, classify, track and manage USC-owned hardware information assets. For the purpose of this policy, "USC-Owned" is defined as any hardware asset procured by a USC-affiliated party for the primary purpose of accessing, storing or processing USC information.

Policy Requirements

5.1 Asset Custodian will identify and maintain an up-to-date inventory of all USC-Owned hardware assets which they procure and provision in association with information and information processing (e.g., equipment).

5.2 The asset inventory will identify the following at a minimum: Asset Custodian, Asset User (assigned to), physical location, OS type, Asset Name, Asset Manufacturer, serial number, asset tag (if applicable), MAC address and group or unit of each asset.

5.3 As requested, the asset inventory will be reported to OCISO.

5.4 Asset Custodian will ensure that assets are classified and labeled based on their importance and sensitivity of the data that resides on each device, using the defined classification terms in the Data Protection Policy.

5.5 Asset Custodian will identify, document, and implement rules for the acceptable use of information and of assets associated with information and information processing facilities.

5.6 Asset Users will protect their assets from loss, damage, misuse, and unauthorized access to a level commensurate with the device classification and the Endpoint Security Policy.

5.7 Asset Custodian and Asset Users will implement adequate procedures for the protection of removable media.

5.8 Asset Custodian will implement adequate protections to assets, in accordance with the Endpoint Security Policy.

5.9 Asset Custodian will ensure that devices are returned from the Asset Users upon termination of their employment, contract, or user agreement for the particular device.

5.10 Asset Custodian will ensure that assets are securely decommissioned, based upon a defined industry standard, at the end of useful life and that the asset is removed from the asset inventory.

5.11 Document your Asset Inventory and validate that it meets the minimum requirements of the OCISO Asset Inventory template.

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