Technology Asset Management Policy

Policy Contents

I. POLICY STATEMENT
II. REASON FOR POLICY
III. SCOPE
IV. AUDIENCE
V. POLICY TEXT
VI. PROCEDURES
VII. RELATED INFORMATION
VIII. DEFINITIONS
IX. FREQUENTLY ASKED QUESTIONS
X. REVISION HISTORY
XI. COMPLIANCE
XII. POLICY EXCEPTION PROCESS
XIII. APPENDICIES

Effective Date: 03-01-2015
Last Updated: 02-18-2015

Responsible University Officer:
Opinder Baw
Vice President, Chief Information Officer

Policy Owner:
Director, Client Support Services

Policy Contact:
ITS Help Desk
I. POLICY STATEMENT

A. The Desktop Computing Subcommittee reviews the latest desktop and laptop technology and approves USF hardware and software standards that meet the needs of most of the University. ITS provides full support for standard equipment approved by the UITC.

B. University-owned Technology Assets (see definition below) are required to have a USF Inventory Tag. Inventory tags are recorded and tracked by ITS. The inventory tag must be attached by an authorized ITS Staff member.

C. Computer Names, also known as "Host names," are based on the USF Inventory Tag number. Host names must not be changed on desktop and laptop computers.

D. All vendor decals, stickers and other serial number identifiers must not be removed. Serial numbers and model numbers are recorded and tracked by ITS.

E. All University-owned technology assets must be assigned to an individual with full-time, permanent employment status with the University. This person is referred to as the asset responsibility owner.
   - Assets used by temporary or part-time staff and faculty must be assigned to an appropriate full-time, permanent asset responsibility owner. The responsibility owner must indicate that the asset will be used by a temporary staff or faculty member. The temporary staff or faculty member will be identified as the "Primary Client".
   - USF asset responsibility owner information and Primary Client information are recorded and tracked by ITS.

F. Responsibility owners of University technology assets cannot exchange, trade or "cascade" assigned equipment without notifying ITS and receiving approval from the UITC chair (uitcchair@usfca.edu).

G. All University-owned technology assets must have a campus location. The location must have an exact campus address that includes an Office Number or Cubicle Number if applicable.
   - Assets that are intended for university-related travel or "virtual" office are still required to have a campus location of record. The location should indicate where the asset will be located most often and would be brought in for servicing or replacement.
   - Location information is recorded and tracked by ITS.

H. Department Supervisors and Managers are responsible for returning any unwanted or unneeded assets to ITS. These assets will be assigned and re-purposed to other areas of the University.
I. All University-owned laptops and public computers must have a security cable-lock. Please refer to the Laptop Cable Locks Policy and Procedures.

J. All University-owned computers must have the LANDesk Management Agent installed. The LANDesk agent ensures the Asset Management System is updated with current information. The agent operates transparently on the client's computer with no performance impact.

K. USF Asset responsibility owners of computer assets must connect their computer to the USF Network at least once a month to receive software security patches and antivirus definition updates.

L. All University-owned computers must be "joined" or bound to the USF Active Directory for authentication purposes.

M. All assets that have reached the end of their useful life (e.g. failure, replacement, etc.) will be decommissioned per the procedures described in the Computer Retirement Policy.

II. REASON FOR POLICY

A. The purpose of this policy is to create an authorized process for managing technology assets (computers, monitors, software, etc.) purchased through the University of San Francisco's Refresh Program (RP) budget.

III. SCOPE

A. This policy covers all technology assets (computers, monitors, software, etc.) purchased through the University of San Francisco's Replacement Program (RP) budget.

IV. AUDIENCE

A. Coordinators, technical liaisons and budget approvers from each Division/School/College need to adhere to this policy. ITS staff responsible for technology asset management shall also adhere to this policy.

V. POLICY TEXT

A. Objectives

1. Efficient use of University resources: This policy is designed to support the implementation of internal inventory control procedures, asset management processes and general tracking of USF computer assets.

2. Support existing USF Computer Retirement Policy Objectives:
Compliance with applicable laws: Laws such as Gramm-Leach-Bliley Act (GLBA), FERPA (Family Educational Rights and Privacy Act) and HIPAA (Health Insurance Portability and Accountability Act) require that the University safeguard confidential information which may be stored on desktop and laptop computers. This requires that all computers be re-inventoried and de-provisioned by ITS.

Compliance with EPA (Environmental Protection Agency) regulations: The University must ensure that all computers are responsibly disposed.

3. Provide complete, accurate financial audit capabilities for technology assets as needed by the Business & Finance division, Internal Audit, or third-party auditors.

4. Optimize Software Purchases:
   - Provide the University the ability to identify and analyze commonly installed software (e.g. analysis of "single license" software purchases versus "site license" volume agreements).
   - Comply with Software Licensing Policies: Provide the University with an authorized process for verifying compliance with centrally-managed client software agreements (e.g. report on number of Microsoft Office licenses currently installed).
   - Centrally identify, manage and proactively provide software updates and security "patches" to the University.
   - Centrally distribute new software packages.

5. Provide the University with information to track assets that have been reported stolen, lost or missing.
   - Support USF Public Safety police reports

6. Support the University's Information Security Policy.

7. Provide ITS with information to aide troubleshooting and support.

VI. PROCEDURES

A. (None)

VII. RELATED INFORMATION

A. (None)
VIII. DEFINITIONS

A. Refresh Program
   1. University of San Francisco's annual technology program that replaces University-owned computers that have reached the end of their useful life. This program has a central budget.

B. Technology Assets
   1. Assets owned by the University of San Francisco that consist of the following equipment types:
      • Desktop Computers
      • Laptop Computers
      • Servers
      • Projectors
      • Printers
      • USF Standard Software

   Note: Fax machines, copiers and other equipment are beyond the scope of this policy.

C. LANDesk Agent
   1. A small application that inventories installed software and hardware devices. This software does not track web usage, e-mail or files.

D. Computer Retirement
   1. After a University-owned computer reaches the end of its useful life, the computer must be properly removed from the campus network and all data contained on the hard drive must be destroyed (wiped).

E. UITC
   1. University Information Technology Committee

F. Desktop Computing Subcommittee
   1. USF's IT Governance subcommittee that oversees the maintenance and development of USF's desktop computing environment.

G. FERPA
   1. The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

H. GLBA
I. HIPAA
   1. Health Insurance Portability and Accountability Act is a federal regulation establishing national standards for health care information.

J. Software Policy
   1. Unauthorized copying or installation of software.

IX. FREQUENTLY ASKED QUESTIONS
   A. (None)

X. REVISION HISTORY
   A. 04-15-2013 – First publication of policy
   B. 03-01-2015 – Updated to use the new format

XI. COMPLIANCE
   A. Failure to follow this policy can result in disciplinary action in accordance with Human Resources Employment Handbook and Office of General Counsel employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS
   A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
   B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
   C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
   D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES
   A. (None)