Technology Asset Management Policy & Mobile Device Management Policy

The purpose of this policy is to create a process for managing the technology assets (computers, mobile devices, software, etc.) of the UTSA Office of Facilities.

Policy Objectives
The objectives of The University of Texas at San Antonio Office of Facilities Technology Asset Management Policy are as follows:

1. Efficient use of Facilities technology resources: This policy is designed to support the implementation of technology inventory control procedures, asset management processes and general tracking of UTSA Office of Facilities computer assets. This is to augment, not supersede or replace University processes and procedures. It also does not supersede budget and purchase authority as defined by University and Office of Facilities policies.
2. Support the University's Information Security Policy especially as it applies to network-connected devices and mobile devices.
4. Provide complete and accurate information regarding location, cost, and assignment of technology assets as needed by Office of Facilities management.
5. Optimize Software Purchases:
   - Ensure compliance with purchased software license agreements
   - Provide the ability to identify and analyze investment in software across the Facilities organization (applications unique to departments or specific job duties, applications needed by the majority of Facilities employees, special project software, etc.)
   - Provide identification and support for software updates and security "patches" specific to Facilities technology assets (in support of updates provided by OIT)
6. Provide Business Services with information to aide troubleshooting and support.

Scope
This policy covers University-owned desktop, laptop, and tablet computers; University-provided “smart” phones; network-attached printers; University-owned external data storage; and software licenses. Mobile devices (tablets and smart phones) are covered in Appendix A of this policy. University-provided mobile phones without data capabilities, radios, and copiers are not included in the scope of this policy.

Technology Asset Management Policy
Technology Standards
Facilities Business Services will maintain a list of supported hardware and software. This list will be periodically reviewed by the Information Technology Working Group (see definitions...
below) and changes will be recommended as appropriate. Recommendations from the Working Group for changes to approved technology hardware and software are presented at the beginning of each calendar year to the Facilities Senior Executive Team (SET) and approved by the Associate Vice President of Facilities (AVPF). Status of installed technology and related Facilities automation issues will be reviewed by the SET and AVPF on a monthly basis.

**Acquisition and Re-deployment**

Business Services will provide support and advice to Facilities department management to address new or changing technology requirements. Existing equipment will be re-purposed when appropriate or new systems will be specified if existing systems do not support defined business needs. The respective department management will identify funds to be used to acquire or modify technology assets that are not already part of an existing technology program.

**Support**

Approved hardware and software receive support from Business Services. Non-standard technology will be reviewed by Business Services prior to purchase to ensure that adequate support is available through Business Services, OIT, or a contracted support organization. If a support mechanism is not available, the end user will be encouraged to seek an alternate solution that can be supported.

University-owned Technology Assets (see definition below) are recorded and tracked in the Office of Facilities' computerized maintenance management system (CMMS), currently WebTMA. This system and the associated work control processes are used to track corrective maintenance, technical support requests, changes in hardware or software configuration, and re-location/re-assignment of the asset.

Any technology asset support, purchase, upgrade, or disposal requests will be submitted via the iService Desk web application or by phone call to Facilities Work Control. Business Services will provide support in a timely manner for all approved hardware and software. Limited support will be available for non-standard technology but Business Services will assist the end user in obtaining solutions when requested.

**Responsibility Owner**

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. In the case where an asset is used by temporary or part-time employees or student worker, an appropriate full-time employee (preferably the supervisor of the part-time employee) will be assigned as the Responsibility Owner. In these cases, the end user of the equipment will be listed as Primary User in the database as separate from the Responsibility Owner.

Asset Responsibility Owner information and Primary User information are recorded and tracked by Business Services in the WebTMA CMMS database.

Business Services is responsible for relocation, exchange, trade, or re-purposing Technology Assets within the Office of Facilities. Requests to change the location or assignment of a
Technology Asset will be submitted to Business Services via iService Desk. Re-location or change in assignment require at least director-level management approval.

Location of Assets
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 as appropriate.

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. An electronic copy of the completed and approved “Removal of Equipment” form will be attached to the asset record in WebTMA. Location information is recorded and tracked by Business Services in WebTMA.

Disposal
Department Supervisors and Managers are responsible for returning any unwanted or unneeded assets to Business Services. These assets will be assigned and re-purposed to other areas of Facilities if possible or sent to Surplus if the equipment is judged to be obsolete or if repairs are too costly. University policies and procedures regarding surplus assets will be strictly adhered to.

Security and OIT Policies
Security measures such as password-protected access, limited local storage of University information, encryption of data, and secure storage of portable devices are to be applied per UTSA Office of Information Technology (OIT) policies and procedures.

For Microsoft Windows and Apple OS devices, Responsibility Owners of computer assets must connect their computer to the UTSA Network at least once a month to receive software security patches and antivirus definition updates. Similarly, all University-owned computers must be "joined" or bound to the UTSA Active Directory for authentication purposes when the operating system of the device supports it.

Tablet systems (e.g., IOS and Android-based devices) require secure password protection and proper storage when not in use. Business Services will apply encryption and other security measures as they are developed and supported by UTSA OIT.

Policy Exceptions
Only the Associate Vice President of Facilities approves exceptions to this policy.

Definitions
PC Replacement Program – The Office of Facilities PC Replacement Program replaces University-owned computers that have reached the end of their useful life as annual funding allow. This program has a central budget managed by Business Services. Per this policy, exceptions to the PC Replacement Program require AVPF approval.

Technology Assets - Assets owned by The University of Texas at San Antonio that consist of the following equipment types:

- Desktop Computers
- Laptop Computers
- Tablets (regardless of operating system)
- Servers
- UTSA Office of Facilities Standard Software
- Network-attached printers
- UTSA purchased external storage devices (with capacity greater than 100 GB).

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

**Information Technology Working Group** - Business Services will coordinate an IT Support committee to ensure good service and responsiveness to changing requirements. The committee is made up of one representative from each of the Facilities production and support departments. It is chaired by the Director of Business Services or their appointee.

**Technology Asset Disposal** - 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). Procedures of the University's Surplus Property department are followed when technology assets are disposed of.

**Software Piracy** - unauthorized copying or installation of software.
Mobile Device Management Policy

Policy Objectives
This part of the UTSA Office of Facilities Technology Asset Management policy addresses issues specific to mobile computing devices.

Scope
This policy covers mobile devices owned by The University of Texas at San Antonio consisting of the following equipment types:
- Tablets (regardless of operating system)
- Smart phones (iOS, Android, and Blackberry)
- Notebook computers running Android-based operating systems

Mobile Device Management Policy
Mobile Device Standards
Facilities Business Services (FBS) supports University-owned Apple mobile devices and select Android-based tablets in use by Office of Facilities personnel. Support for additional devices will be added as required.

Responsibility Owner
As technology assets, University-owned mobile devices must be assigned to a Responsibility Owner (an individual with full-time, permanent employment status with the University). See the Technology Asset Management policy for information about this role.

Security
Mobile Device Management System
All mobile devices issued by the Office of Facilities will be required to be “enrolled” in a Mobile Device Management (MDM) system. This system provides additional security as well as consistency to the applications and data stored on the mobile device. End users of the devices are not to tamper with the settings of the MDM software installed on their assigned devices.

FBS will use the MDM system to apply password restrictions, encryption, and other security measures to mobile devices. These security measures will be modified as needed to meet University of Texas and UTSA security guidelines as they are developed. Since not all mobile devices are considered part of the University asset inventory, Facilities Business Services (FBS) will maintain an inventory of mobile device hardware in WebTMA that includes device serial numbers and the assigned Responsibility Owners.

Location of Mobile Devices
All University-owned mobile devices must have a campus location where they are stored when not in use. The Responsibility Owner is required to securely store the mobile device in this location. The location must have an exact campus address that includes an Office Number or Cubicle Number as appropriate.
Disposal
Department Supervisors and Managers are responsible for returning any unwanted or unneeded mobile devices to FBS. University policies and procedures regarding surplus assets will be strictly adhered to.

Exchange and Trade in
Responsibility Owners of mobile technology assets cannot exchange, trade, or "cascade" assigned equipment to other employees or departments without notifying FBS and receiving approval from the Responsibility Owner’s Director or Assistant Vice President. Mobile devices turned into Facilities Business Services will be erased prior to re-assignment or surplus. Department Supervisors and Managers are responsible for removing University information from these devices prior to surrendering them. If the mobile device is to be disposed of, it will be properly removed from the campus network and all data contained in it will be completely removed ("wiped").

Policy Exceptions
Only the Associate Vice President of Facilities approves exceptions to this policy.

APPROVED:

Dave Riker
Associate Vice President for Facilities

DATE: 5/8/14