Information Technology Asset Management

Purpose:

The purpose of this document is to provide guidelines for lifecycle management of the ASU technology assets for procurement, installation, management and surplus salvage.

1. **General**

    a. ASU uses information technology to assist the organization in achieving its objectives.

    b. Technology, as defined by the Office Code of the State of Georgia, includes, but is not limited to hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology. Related consulting services shall also be included within this definition. (O.C.G.A. § 50-25-1.)

    a. The ASU Office of Information Technology (ASU-OIT) is responsible for the management of electronic and technology assets and lifecycle processes, including standards, acquisition, management, surplus, and long-range planning.

    b. Consistency in technology allows the development of efficient and cost-effective methods for supporting and managing the technology environment and in planning for upgrades, migrations, staff training, and future technology installations. Long-range planning for information technology changes shall include business as well as technical input.

    c. Technology assets acquired for or on behalf of ASU is owned by ASU.

    d. Electronic and technology equipment is assigned to the position, not the individual, and remains with the position if the individual terminates employment or is transferred to another position. If a position is abolished, IT equipment will be returned to ASU-OIT inventory.

    e. Technology equipment will be used within ASU as long as practicable.

    f. Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

2. **Acquisition**

a. Acquisition of all information technology for ASU is the responsibility of the Chief Information Officer (CIO). Authority to acquire technology may be delegated by the CIO.

b. Acquisition of IT shall follow a central purchasing method. Purchases, contracts, amendments, and renewals will be processed through ASU-OIT for approval by the CIO or designee.

   i. **Procedure.** Departments shall request procurement action by ASU-OIT by means of electronic or written requests.

   ii. **Verbal Requests.** Verbal requests for procurement activities are not satisfactory substitutes for electronic or written requests except in emergencies. Electronic or written confirmation must follow any such request made in an emergency situation.

   iii. **Confidentiality.** All information and documentation (verbal and written) relative to development of a contractual document for a proposed procurement shall be deemed confidential in nature, except as deemed necessary by the purchaser to develop a complete contractual document. Such material shall remain confidential until successful completion of the procurement process.

c. Approvals for acquisition are based on availability of funds as determined by the CFO's designee, conformance to IT standards, and solution match for business need.

d. All IT acquired for or on behalf of ASU or developed by ASU-OIT employees or contract personnel on behalf of ASU are and shall be deemed ASU property.

3. **Standards**

a. A standard, basic technical infrastructure will be established for ASU. It will be defined and managed by ASU-OIT and will include the network and the desktop.

b. Desktop IT consists of standard hardware and software configurations and images (excluding test computers).

c. ASU-OIT is responsible for:

   i. Establishing hardware and software standards for any IT product.

   ii. Reviewing requests for new, amended, or replacement IT standards. New-to-ASU IT will be assessed by ASU-OIT staff for compatibility with and impact on other ASU IT components, as appropriate.

   iii. Using department-wide business and technical needs in determining approval of new, amended, or replacement standards.

   iv. Establishing standard software configurations and desktop images. These standards shall automate business rules where possible (e.g. use of screen saver password protection).

v. New IT policy and standard decisions shall have formal plans for implementation.

4. **Equipment Management**

   a. ASU will control its IT assets to comply with State policies and regulations, as well as applicable licensing and copyright laws.

   b. ASU-OIT is responsible for tracking ASU-owned software and hardware, including licenses, through an inventory control system (ASU-OIT will utilize Track-IT ©, which will track IT hardware and software inventories). Software inventory records and reports shall be available in accordance with ASU ASU-OIT policy. All software licenses (or copies of the licenses, purchase orders, or copies of VISA statements with software purchases highlighted) will be sent to the CIO's office for central tracking and control.

5. **Installations of Software and Hardware**

   a. ASU shall maintain an IT environment whereby installations and configurations are centrally managed through ASU-OIT.

   b. Only ASU designated standard software, hardware, or approved exception shall be installed.

   c. Software, hardware, or approved exception must be ASU owned or licensed. All software without required licenses will be removed from the desktops/laptops.

   d. Designated ASU-OIT staff shall authorize installations of software, hardware, or approved exception.

   e. Installation of business-related, no cost software (i.e. Adobe Acrobat Reader or browser-required applications) shall be approved through ASU-OIT. These types of software shall be evaluated through the standards and exception to standards procedures.

   f. User-supplied software shall not be installed or executed on ASU-owned desktops. Do not install or connect non-ASU hardware to an ASU network.

   g. Unauthorized duplication of licensed software is a violation of this policy and a violation of copyright laws.

   h. All excess IT equipment within ASU shall be the responsibility of ASU-OIT to reuse or surplus as determined by ASU-OIT. First priority for redeployment requests within ASU shall be with the business unit where excess equipment originated.

   i. ASU-OIT shall delete all data and applications, exclusive of the operating system, from all excess IT equipment prior to re-deployment or placing in spare inventory, loans, or surplus.

   j. ASU-OIT shall be responsible for delivery of equipment to the identified re-deployment work site.

k. ASU-OIT shall store spare IT equipment in a designated reserve location for use as needed.

6. **Exceptions**

a. ASU-OIT is responsible for reviewing and approving exceptions to IT policies.

b. ASU-OIT may grant exceptions to this policy under extraordinary circumstances. Requests for exceptions must be made in writing to ASU-OIT stating the business need and unique circumstances requiring an exception.

c. ASU-OIT will evaluate and determine if the requested exception can be reasonably resolved through technology within the confines of the ASU technology environment.

d. For granted exceptions, the requester must establish with ASU-OIT a plan for technical support, training, and maintenance. The plan shall be developed prior to purchase or implementation of non-standard technology.

e. Exceptions shall be considered provisional and can be superseded any time an ASU standard is determined. If a broader need is determined at the time of an exception request, then an ASU standard will be established.

f. Upon granting an exception regarding access to or connection with the ASU local or wide area network, a written agreement between the requester and ASU-OIT must be developed stating the conditions of access, security, technical support, and maintenance.