Technology Acquisition Policy

**Functional Area:** Information Technology Services (IT Services)  
**Date Issued:** January 20, 2014

**Applies To:** All employees and third-party vendors  
**Date of last review:** January 20, 2014

**Policy Reference(s):**  
Data Classification Policy  
Responsible Access and Use of Information Technology Resources and Services (Section 4)  
**Date of next review:** July 1, 2014

**Page(s):** 2

### Responsible Person

This policy will be re-evaluated on or about the first day of July each calendar year to determine whether all aspects of the policy are up to date and applicable in the current business environments, and will be revised as necessary. The Chief Information Officer is responsible for the review and accuracy of this policy.

### Purpose / Rationale

To ensure that resources (monetary and staff time) are used as effectively as possible and that data security standards are protecting university data, all acquisitions of technology hardware, on-site software, software as a service (SAAS or “cloud”) or consulting contracts.

### Definitions

**SAAS** is the acronym for Software as a service, sometimes referred to as "on-demand software" supplied by ISVs or "Application-Service-Providers", is a software delivery model in which software and associated data are centrally hosted on the cloud.

**Cloud** refers to the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

**Enterprise-level software** also known as enterprise software application (ESA), is purposed-designed computer software used to satisfy the needs of an organization rather than
individual users.

**Functional business owner** is the person responsible for defining the way in which an IT resource is used. Defines the activity, purpose, or task; relating to the way in which something works or operates.

**Mission critical system** is a system whose failure or malfunction will result in not achieving organization goals and objectives. The principle of Least Privilege (PoLP) describes minimal user profile or access privileges to information resources based on allowing access to only what is necessary for the users to successfully perform their job requirement.

**Service Level Agreements** (SLAs) can be separate from but complementary to a signed contract that governs the delivery of services between providers and Armstrong.

---

**Policy**

This policy seeks good stewardship of the university’s resources by managing cost through standardizing where possible and ensuring flexibility to meet the academic mission. To ensure that resources are used as effectively and efficiently as possible and that data security standards are protecting university data:

1. IT Services will maintain a list of pre-approved technology items including but not limited to computers, laptops, tablets, and printers that will not require additional approval to purchase.

2. All other acquisitions of technology hardware, on-site software, software as a service (SAAS or “cloud”) or consulting contracts must be reviewed and approved by the CIO, or his/her designee, prior to purchase or renewal based on the following characteristics:
   - If the purchase amount is over $1,000, or
   - If the ongoing maintenance cost of the hardware, software, or service is over $500 per year, or
   - If the acquisition is for computers, laptops, tablet, and printers not on the pre-approved list, or
   - If the acquisition will access or store sensitive or confidential data, including but not limited to student data, health records, or financial data (see Data Classification Policy), or
   - If the acquisition will require access to a server or network resource, or
   - If the acquisition requires IT Services assistance to implement or support.

   Note: While scientific research or teaching equipment that does not connect to the network or store sensitive information is excluded from the approval process, it is highly recommended that IT Services be involved in the acquisition process to ensure that technology purchase(s) can be supported by our infrastructure.

3. If software or services require authentication and can be tied into Armstrong’s single sign-on infrastructure and methodology, then the acquisition or renewal must include these components.

4. Typically, enterprise-level software and services are continuously changing through revisions and version changes. Therefore, enterprise-level software or services must be reviewed every three to five years by the functional business owner and IT Services to determine if functionality and cost align
with the university’s strategic goals.

5. All third-party software or service providers will be required to enter into a service level agreement with Armstrong. All SLAs will define overview, goal and objectives, service description, stakeholders, review periods, service agreements, and service management including performance metrics, uptime, response time, remediation, and access guidelines.

6. IT Services recommends keeping software and services under a current maintenance contract, patch level, and current release. For mission critical software services or when IT Services is responsible for providing support, software and services must be covered by a maintenance contract, patch level, and current release.

7. IT Services recommends initial user training during acquisition of software or services and continued training throughout the life cycle of the software or service.

Any exceptions to the above require written justifications for review and approval by CIO.

Nothing in this policy should be construed to supplant the special jurisdictions and procedures set forth by federal or state laws or USG policies.