Technology Acquisition Life Cycle Management Policy

Updated and Effective of: 10/1/2016

Responsible University Officer: Vice-President, Chief Information Officer (VP-CIO)

Policy Owner: Associate Vice-President, Information Technology

I. Purpose

The University’s information assets are essential resources in delivering the University’s core mission. These assets include information and communications technology equipment (e.g., hardware and operating systems), software used on University provided computers, multi-user or enterprise applications hosted on University owned servers, and applications and services provided by external Third-Party vendors that store, access, process, or transmit University data.

It is University policy to manage these assets across each phase of their life cycle: plan and acquire; configure and deploy; maintain, support and upgrade; decommission, retire, and dispose. Each phase must include the approval of the VP-CIO, or designate, to ensure the assets conform to standards addressing technology architecture, information security, service delivery, service operation, refresh, disposal, and license management.

By implementing this policy the University will:

a. ensure that appropriate information security standards, practices, and controls are included and applied during all phases of an asset’s life cycle,

b. ensure conformance with appropriate technology architecture, service delivery, service operation, and license management standards,

c. ensure proper removal of data and licenses when an asset is re-purposed, retired, or disposed,

d. integrate life cycle management into the asset acquisition or implementation processes and require VP-CIO, or designate, approval for any asset that stores, accesses, processes, or transmits University data,

e. prevent the introduction of new information security risks when an asset is modified, undergoes significant change, is upgraded, or retired,

f. ensure information, data, and technology assets are regularly backed up and critical IT assets are included in an IT disaster recovery plan,

g. comply with Federal, State, local laws and regulations, University policies, and applicable agreements binding the University,

h. ensure this policy is consistently applied and monitored through the use of a compliance program.
II. Scope

- This policy applies to all Divisions, Schools, and Colleges, and members of the University community in all campus locations identified as the owners of assets that create, access, store, process, or transmit data and information. This includes assets purchased, licensed, or contracted by the University that are either centrally funded or grant and special account funded whether running in the University data center and network, or provided externally by a Third-Party.

III. Responsibilities

a. The Vice-President, Chief Information Officer (VP-CIO) designates the Associate Vice-President Information Technology (AVP) to be responsible for the development and maintenance of this policy.

b. The VP-CIO is responsible for approving and ensuring ongoing compliance with this policy with oversight from the Board of Trustees (BoT) Committee on Information Technology Strategy (CITS).

c. The University Leadership Team are responsible for championing this policy and supportive information security practices in their respective Divisions, Schools, and Colleges, and any substantive revisions, as recommended by the VP-CIO.

d. The VP-CIO is responsible for ensuring information assets acquired or implemented under this policy are secure from unauthorized access (to maintain appropriate confidentiality), unauthorized alterations (to maintain integrity), and available to authorized Users (to maintain availability) enabling the University to meet its mission in an effective and timely manner. The VP-CIO may delegate responsibility for this policy to the AVP.

e. The AVP is responsible for incorporating, and maintaining, reasonable security processes, practices, procedures, guidelines, and technologies into the life cycle of an information asset, and ensuring that this policy is reviewed and updated as necessary.

f. The Information Security Officer (ISO) is responsible for establishing and maintaining an information security program to support this policy, and for coordinating with the AVP on the ITS response to information security incidents, violations, or crimes committed under this policy.

g. All Users are responsible for being familiar with, and complying with, this policy. Users involved in the acquisition, implementation, and management of an asset have individual and shared responsibilities to comply with this policy to protect the confidentiality, integrity and availability of the information asset in accordance with University policies, Federal, State, local laws, regulations, and agreements binding the University. Users are required to take information security and awareness training appropriate to their role.

h. Users should seek further guidance from the AVP if they are unsure of their responsibilities under this policy.

i. The Office of the General Counsel will provide legal guidance to this policy.

j. Failure to comply with this policy can result in actions to limit, suspend, or revoke access to the University’s network, email, and other information assets. Members of the University community who knowingly violate this policy may be subject to disciplinary actions that
include but are not limited to the policies and procedures contained in the Staff Handbook, the Student Handbook (Fogcutter), applicable Collective Bargaining Agreements, and laws which may include civil and criminal prosecution.

IV. See Related Policies

a. Electronic Communications Policy.
b. Information Security Policy.
c. Technology Resources Appropriate Use Policy.