Asset Safeguarding Recommendations for AMC

All IT and related equipment must be kept in rooms that are locked and/or supervised by state employees at all times. Whenever a user leaves and/or a room is unattended the user will be required to leave their IT equipment in a "secured state".

A "Secured state" is one in which the IT equipment is secured both physically and electronically. The physical requirement will be met when the equipment is locked down with a connected security lockdown device (cable and lock, security bracket, etc.) or stowed away in a secured/locked drawer or cabinet. The electronic requirement will be met when the equipment complies with the recommendations in the Electronic Security section below.

Physical Security:
Best practices:

Laptop:
All laptops should be protected with a S.T.O.P. plate to help deter theft and promote the chance of recovery if/when identified.
Whenever laptops are left unsupervised in a locked office, they must be stored in a locked drawer or cabinet.
As laptops are designed to travel with their user, cable locks may not always be required but will be required when the laptop is regularly left in an unsupervised office.

Desktop:
All desktop computers and their corresponding displays should be physically locked down with a cable lock.

Printer:
All printers over a determined value (e.g. $400) should be physically locked down with a cable lock.

Electronic Security:
Best practices:

All computers in AMC should be encrypted with the appropriate vendor provided encryption application (Filevault for Apple and BitLocker for Windows) and the decryption key should be stored with the Dean's Office and department area techs. Further user training would be required as system changes can sometimes spark a request for the encryption key (USB drives for example, so an additional set of recommendations for data backup per the user and per the College will need to be developed and provided).

All computers in AMC should be on the campus Active Directory except when not feasible, and MUST in all cases require a screensaver and password to unlock them after a system suspension (e.g. sleep/hibernate).

All computers in AMC that work with "important data" or "secured data" should either be backed up routinely to a Department/College/University server or configured to work with such data that is directly stored on said server.

"Important data" is data that either does not/no longer exist(s) in hard copy form, or is data that would cause a measurable hardship for the Department/College/University should it become lost or damaged.
"Secured data" is data such as "Level 1" or "Level 2" which is defined in section 8065.S02 of the Information Security Data Classification Standards (http://calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf)

All computers in AMC should be maintained with a current set of OS and Application updates and patches, including antivirus definition files per the Information Security Configuration Management Standards, section 8050.S100, 1.4; and Section 8045.S200, 1.2d (http://www.calstate.edu/icsuam/documents/Section8000.pdf)