UNIVERSITY OF MASSACHUSETTS/AMHERST
INFORMATION TECHNOLOGY ACQUISITION AND LEASE REVIEW CHECKLIST - Instructions

All hardware, software, applications, leases and services are subject to an Information Technology (IT) review to ensure compliance with federal, state and university policies. This checklist applies to all new IT purchases as well as existing systems that undergo substantial contractual, functional, or operational changes

Section I
Hardware – this section is for any piece of hardware you are purchasing but not for consumable computer supplies such as tapes for backup, cables, mice, etc. If your entire purchase is hardware and falls into Section I, you do not need to fill out Section II unless the purpose of the hardware purchase is to store or transmit sensitive data. In those cases, you must answer the questions in Section II. Please note that all hardware should have a commodity code of *Equipment – Information Technology* regardless of cost.

Section II Explanation
These questions must be answered for any purchase including hardware not listed above, for example: servers. If any of the questions in this section apply you must choose the commodity code of ***UMAMH IT Procurement Review Admin*** for administrative departments or ***UMAMH IT Procurement Review Academic*** for any academic department.

1. Will the purchase store, transmit, or process any sensitive data (credit cards, FERPA, HIPAA, SSN, etc)?
    a. Any data that is protected under, but not limited to, FERPA, HIPPA, MGL 93H, PCI needs to have specific contract terms associated with the purchase. In addition, your network, workstations and laptops that will access this information may need to have additional controls on them to be compliant under these rules and statutes.
    b. If you are not sure what you are storing or transmitting is sensitive data, submit the purchase for review. Sensitive data that do not have sufficient protections and are breached could result in large fines to the University and the affected department.

2. Will the purchase process credit card transactions or have the capability to process credit card transactions?
    a. All credit card processing must be approved by the campus eCommerce representative as the University has specific requirements around credit cards for us to remain complaint under Payment Card Industry Standards. In some cases, there may already be a solution you can take advantage of. See http://www.umass.edu/afsystems/basic-page/ecommerce/95 for more information.
    b. Contract terms will be required by the University to ensure the vendor provides sufficient protections.

3. Will any UMass data be stored 'in the cloud' or in a vendor hosted environment?
    a. This question does not apply if you are storing your data in the University's Google Apps. As part of getting access you acknowledged being informed not to store sensitive data.
    b. Depending on the type of data you are putting "in the cloud" a detailed system review may be required by OIT to ensure appropriate protections.
    c. Contract terms are required to ensure the vendor provides sufficient protections. There may also be specific prohibition against using certain resources (authentication, data interfaces, etc) if the service is located off campus.

4. Will the purchase require a data interface between SPIRE, HR, Finance, or any other enterprise data source?
    a. Requires data custodian approval of the system from which you want to interface data
    b. If this requirement means programming from OIT for SPIRE or UITS for HR or Finance data, you need to go through the appropriate channels to request the information and to make sure resources are available to meet your timelines
    c. Contract terms are required to ensure the vendor provides sufficient protections.

5. Will the purchase utilize the Ucard iClass prox, magstripe or barcode in any way?
    a. The Ucard has a variety of ways for someone to present data to prove who they are but not all are at the same technological level and are being phased out. MagStripe, for instance, will eventually be phased out and replaced via the University iClass prox technology on every card. Any new system that would assume to use the Ucard as an identifier needs to contact the Ucard office concerning their needs.

6. Will the purchase require any consultation or professional services that may have access to sensitive data?
    a. Requires data custodian approval of the access to sensitive data.
    b. Contract terms are required to ensure the vendor provides sufficient protections

7. Will the purchase require using the campus NetID to login?
    a. If your purchase will need to use Shibboleth or the campus LDAP to authenticate people, it will require OIT Information Security approval. This does not apply to use of your NetID to login to the campus network on a desktop or laptop or to access existing campus resources.

8. Will the purchase be required for critical business processes?
    a. In Disaster Recovery/Business Continuity (DRBC) planning terms, is the purchase a critical system needing uninterruptible run time or restoration of less than one week? If management of this critical system requires any resources other than your own department's resources to support "up time", ex OIT networking, the purchase must be reviewed to be sure adequate protections and resources are available.

9. Will the contractor be located off---campus if this is a service?
    a. Contract terms are required to ensure the vendor provides sufficient protections. There may also be specific prohibition against using certain resources (authentication, data interfaces, etc) if the service is located off campus.