# IT USE GUIDELINE

## Software as a Service Purchases

Click here to enter a summary briefly describing the guideline and its use.

## Effective as of: **10/1/2015**

## Sponsor and Approvers:

John McGowan, Scott Montgomery - Sponsors

John McGowan, IT Governance - Approvers

## Status of Guideline: **Published**

## Audience:

This IT Guideline should be observed by:

Students ☐ Faculty ☒ Staff ☒

Contractors/suppliers ☐

Other (specify) ☐ Click here to specify "other".

## Statement of need and purpose:

Not all software available as a service (i.e. hosted on 3rd party premises) is maintained and supported at a level sufficient to ensure adequate information security and intellectual property protections. Alternative solutions may already be available. Some applications may not be easily integrated with the UA network and security architecture. Some applications may impose excessive bandwidth demands on the campus network. This guideline is provided to assist with selection of software services suitable for use by UA constituents.

## Guideline:

1. Understand the risk – Be sure you know what data will be hosted by the application and what potential the impacts would be of data loss or exposure. If there is any personally identifiable information such as social security numbers included, the need for privacy and security is paramount. If the application will host any proprietary information or intellectual property, the risks of exposure or loss must be considered carefully.
2. Understand the services – Ask key questions of the service provider and assure that satisfactory answers are included in the written contract or service-level agreement. These should include but are not necessarily limited to:

   a. What measures does the service provider use to ensure privacy, physical security, backup, and disaster recovery for the data?
   b. Is there a guarantee that the data will not be transmitted through, stored, or copied to storage devices or servers located in any foreign country?
   c. Is the data comingled with data from other "customers" on the same physical hardware?
   d. Is the data encrypted?
      i. When stored?
      ii. During transmission?
      iii. Who holds the encryption keys?
      iv. What encryption standard is used?
   e. What provider employees will have access to the data?
   f. Does the contract assure these policies will be retained even in the event that the company is divested, merged with, or acquired by another company?
   g. What service level guarantees are provided regarding:
      i. Service availability (up-time)?
      ii. Service performance?
      iii. Service problem notifications?
      iv. Incident response?
      v. Incident escalation (how long before, to whom)?
      vi. Frequency of backup or replication processes?
      vii. Time to restore in the event of data loss or system failure?
3. Follow approved contracting processes including:
   a. Engaging UA Purchasing Services
   b. Reviewing technology purchases with OIT
   c. Allowing for legal review of agreements
   d. Ensuring an authorized UA signatory signs any agreements or contracts

## Compliance:

Compliance to Guidelines is voluntary but recommended. Not adhering to guidelines can cause disruption to services, security exposures, and/or adverse impacts to other users. Enforcement of guidelines is addressed when deviations cause issues for others or result in known and significant security exposures and are handled through the organizational management structure.