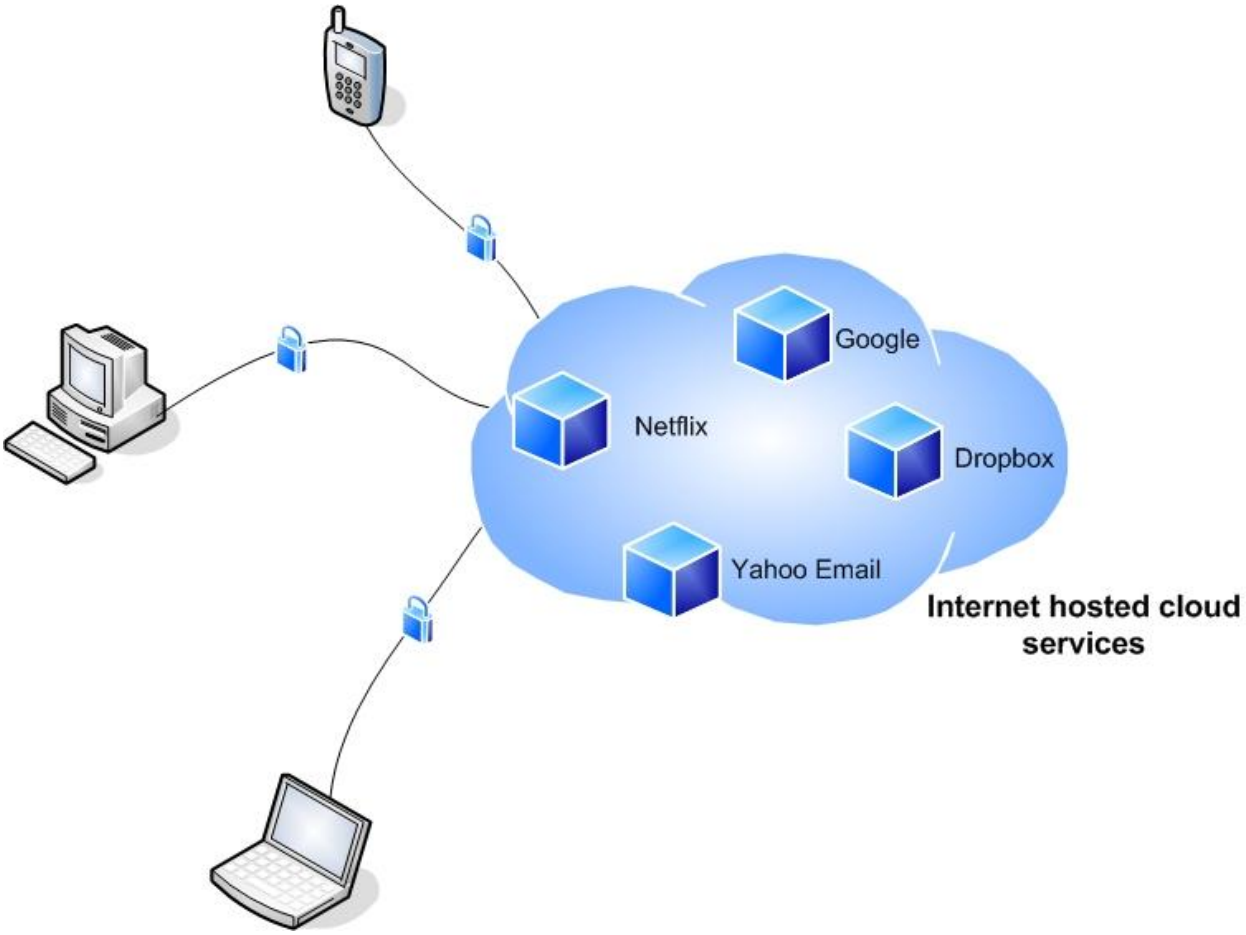

Cloud Services at Notre Dame – Updated 7/16/2012

Cloud services allow the use of applications and data via the Internet using shared systems at remote sites. Examples of cloud services include tools, sites, and applications such as Facebook, Twitter, Google Apps, Prezzi, and Dropbox. These services allow remote storage of data, communications, collaboration, and access to unique tools that may otherwise be too expensive or too specialized to provide to the Notre Dame community.

Cloud services are already used by many organizations and individuals, and Notre Dame recognizes their usefulness for both institutional and personal purposes. Notre Dame has contracted with a variety of cloud services for University use.

Notre Dame Cloud Services Guidelines

Notre Dame requires that cloud services used for University business or data must meet the following requirements:

1. **Licensing:** The license agreement for any cloud service used for Notre Dame business, or to store Notre Dame data must be reviewed and approved by University counsel. Faculty, staff, and students are not authorized to enter into legal contracts on behalf of Notre Dame, and may

not consent to click-through agreements for the purposes of University business. If individual approve these agreements, they would be personally responsible in any legal actions related to the services.

2. **Sensitive Data and Responsible Use:** Use of cloud services must be in compliance with all applicable University policies including:
    a. The *Information Handling Standards*
    b. Notre Dame's *Responsible Use Policy*
3. **Support:** Support of cloud services by Notre Dame (via the OIT Helpdesk, or other support organization) requires prior commitment from the supporting organization.
4. **Data Availability and Removal:** Data stored in the cloud must be accessible and controlled:
    a. Cloud services used for University business must provide the ability to permanently remove University data when desired.
    b. Users are responsible for backing up any data stored in a cloud service.
    c. Users who store University data in any cloud service must make that data available to the University upon request.
5. **Approval**: The use of cloud services for Sensitive data must be approved by an individual holding the position of Associate Vice President, Associate Dean or higher in consultation with Information Security. The use of cloud services for Highly Sensitive data must be approved by both the area's Vice President or Dean **and** the CIO.

Personal Use of Cloud Services

Personal use of cloud services on University owned systems is permissible if the following requirements are met:

1. University data cannot be stored in personal accounts
2. Users must use a different password than that used with their netID
3. If the cloud service requires installation of software on University systems, that software must have its license approved by General Counsel

Cloud Service Reviews

Departments wishing to use a new cloud service for University use must:

1. Undergo General Counsel contract and license review
2. Complete the Cloud Services Provider questionnaire
3. Work with an OIT Relationship Manager and Information Security

Cloud Services Decision Tree