Guidelines for the Use of Cloud Computing Services

University of Scranton
Planning & Information Resources Division

This document provides guidelines for the use of cloud computing services for academic and administrative purposes at the University of Scranton. A list of related University policies is provided at the end of this document for further reference. Departments considering the use of a cloud computing service or other third-party application must contact the Director of IT Development & Applications *before* purchasing the service or application in order to obtain Information Resources' support.

Assistance with selecting cloud computing services is available from IT Development and Applications (ITDA)

IT Development and Applications can assist your department with preparing requests for information or proposals from vendors. Contact Connie Wisdo at x6344.

A 3rd party checklist is available from ITDA containing a list of features and functionality to consider, and precautions to follow, when looking for a cloud service or provider.

What is Cloud Computing?

The term *cloud computing* refers to "the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network" (Educause, 7 Things You Should Know about Cloud Computing, 2009). More practically, we think of these resources as services such as Gmail, Google Docs, Dropbox, WordPress, PayPal, or Flickr that many of us use as everyday conveniences. They have also grown to encompass virtually every area of information technology used in higher education today, including our own email and calendaring tools in Live@edu, learning management and other administrative systems.

There are many benefits to using these services to assist in accomplishing the work of the University. These include reducing costs by only paying for computing resources as-needed, avoiding costly infrastructure investments, gaining work efficiencies in time required to deploy a service, and access to features and functionality that cannot be provided in-house. For these reasons, more and more often Information Resources departments encourage including a review of available cloud services when we receive requests for new IT services.

Challenges with Cloud Computing

The use of cloud computing services also introduce significant concerns related to privacy, information security, data availability and integrity, intellectual property management, and records retention, to name a few (Educause, 2009). Choosing to use a cloud computing service, whether free or paid, to conduct University-related work requires a careful consideration of the following issues.

Terms of Service

Internet applications and service providers often require users to consent to their Terms of Service, frequently via a "click through" agreement — this is a *legal contract*. Students, faculty, and staff are not authorized to enter into legal contracts on behalf of the University and may not consent to click-through agreements for purposes of University business. Individuals who approve these agreements become personally responsible for the terms of the agreement and any problems that may arise.

Terms and conditions contained at a URL should raise a red flag on any contract. It means that terms are subject to change at any time and at the whim of the site administrator. Changed terms could conflict with written terms otherwise in the contract, making that contract difficult to understand and administer. If you need help evaluating an agreement, do not hesitate to contact the Information Security Office or the Office of the General Counsel for assistance.

Tips for Faculty using Cloud Computing Services

Communicate to students the risks and conditions associated with the cloud service you've decided to use at the beginning of the academic term.

Never include personally identifying information about yourself or your students in online content or in profile information

Always require students to use aliases when creating accounts, particularly if access to student work is public. Also prohibit use of my.scranton user credentials.

Privacy & Protecting Identities

The University is mandated by state and federal laws to protect individuals' personally identifiable information; on our campus this information is classified as restricted. Please refer to the Information Classification and Protection Policy at the end of this document for a complete list of restricted and confidential information that must be protected. The security of data uploaded to Internet services is rarely guaranteed. Free services frequently depend on data aggregation and data mining about users to attract advertising revenue. The privacy and security of individual's data is at risk when using these services; you should never divulge information that the University has classified as restricted or confidential on the Internet.

When using a cloud service that is not provided through Planning and Information Resources (PIR) be sure to: 1) comply with all University policies related to protecting privacy; 2) require that students (or others) use aliases when creating accounts, particularly if access to the service is public; 3) restrict access to content to those who need it; and 4) delete any content when it is no longer needed.

Use & Disclosure

The issues, conditions, and risks associated with a computing service or application (not provided by PIR) should be communicated to the individuals who will be impacted, particularly students enrolled in a course or research participants. Students or participants should be allowed to withdraw or participate through alternate means if they have concerns about the privacy of their data.

Other Practical Considerations When Using a Cloud Service

Cloud service providers charge annual fees. Will you be able to pay the annual service/hosting fee(s) out of your department's operating budget?

Will training on the use of the application be needed?

- *Does the vendor provide this service?*
- *Will it be needed on an ongoing basis?*

Will you be using the cloud service to accept payments of any type, particularly credit cards? If so,

- *You will need to be sure that the vendor is compliant with regulations related to credit card payments.*
- *You will need to determine how funds will be directed to the proper University accounts.*

Intellectual Property

It is important to understand who owns the content and what they can do with it when using a cloud service. Review the Terms of Service agreement carefully for provisions about who owns content that is created with or uploaded to the service. Note that cloud computing providers may reserve the right to change their Terms of Service at will. Terms of Service that conflict with the University's Copyright Policy may complicate intellectual property ownership claims.

Data Availability & Records Retention

The University requires that academic and administrative records be retained according to its Records Management & Retention Policy; there are also legal requirements for some records that must be met via this policy. Many cloud service providers assume no responsibility for archiving content or assuring its availability, which places the burden for ongoing accessibility of the data on the individual who approves the service agreement. Also keep in mind that if the cloud service becomes unavailable due to problems with the service itself or connectivity issues, any work processes dependent on the service will have to be performed in an alternate manner.

When using a cloud service that is not provided through Planning and Information Resources (PIR), be sure to: 1) ensure that all records are retained according to University policy; 2) ensure that records can be retrieved from the application or service provider, if necessary; 3) back up materials regularly and have an alternate work plan if the service becomes unavailable; and 4) consider your support needs — the Information Resources division's routine support practices may not be able to resolve technical issues that arise, be prepared to deal with the service provider directly.

This paper discusses only some of the issues that have been encountered in recent years as departments have begun to use cloud services. Again, departments considering the use of a cloud computing service or other third-party application must contact the Director of IT Development & Applications *before* purchasing the service or application in order to obtain PIR support. Please see the related resources and checklist at the end of this document for additional guidance and reference.

Related Resources

7 Things You Should Know About Cloud Computing, Educause (2009)
http://net.educause.edu/ir/library/pdf/EST0902.pdf

Frequently Asked Questions – Cloud Computing
http://www2.ed.gov/policy/gen/guid/ptac/pdf/cloud-computing.pdf

Related University Policies

Information Classification & Protection Policy
Privacy & Confidentiality Policy
http://www.scranton.edu/pir/policies.shtml

Records Management & Retention Policy
http://matrix.scranton.edu/Governance/university-policies%20.shtml

Copyright Policy
http://academic.scranton.edu/department/generalcounsel/policies.shtml

Key Contacts

Director of IT Development & Applications:
Connie Wisdo, x6344 constance.wisdo@scranton.edu

Information Security Office
security@scranton.edu or x5816

Office of the General Counsel
Robert Farrell, x6213 robert.farrell@scranton.edu

Checklist

Cloud computing allows for convenient, on-demand access to computing resources. With Cloud computing, however, come risks that are not associated with normal computing activity (vendor going out of business, location of data storage, legal/intellectual property implications, ownership of data, etc.)

Below is a checklist which will help you assess the potential risks of using a vendor's service. Review this checklist against the vendor's contract/agreement/terms and conditions, as applicable. This is by no means an exhaustive checklist. Refer back to the University's Guidelines for the Use of Cloud Computer Services document for more detailed information and assistance.

DATA SECURITY AND ACCESSIBILITY: Where will the vendor store the University's data?

☐ Pennsylvania ☐ Other US States ☐ Outside of US

DATA SECURITY AND ACCESSIBILITY: Does the vendor back up the data? ☐ Yes ☐ No

If yes, how often does vendor back up the data? ____ times a ☐ day ☐ week ☐ month

Where is the location of the server/data backup? ☐ Same Location ☐ Different Location

LEGAL COMPLIANCE: Does the vendor state that it is fully compliant with applicable laws, regulations, rules or standards, including to the extent applicable, but without limitation to the following?

☐ Family Education Rights Privacy Act (FERPA)

☐ Health Insurance Portability and Accountability Act (HIPAA)

☐ Federal Trade Commission Red Flags Rules (Identity Theft Prevention)

☐ Payment Card Industry Data Security Standards (Sets standards for information security for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards)

INTELLECTUAL PROPERTY: Does the agreement grant the vendor any ownership or publishing rights of the data stored on Cloud? ☐ Yes ☐ No

PRIVACY: Have the privacy risks associated with Cloud computing been disclosed to end users of the service? ☐ Yes ☐ No

Did the end user accept these risks? ☐ Yes ☐ No