Cloud Computing Guideline

Background

This document provides guidance to members of the University of Cincinnati (UC) community who wish to use applications and services available on the Web, including social networking applications, file storage and content hosting. These tools, which often reside on complex, dynamic networks, are collectively referred to as "cloud computing." Refer to Infrastructure, Platform and Software as a Service Policy for additional details related to cloud computing.

Internet Applications

Internet application and service providers may require users to consent to their Terms of Service, frequently via a "click-through" agreement, which is a legal contract. faculty, staff and students are not authorized to enter into legal contracts on behalf of UC and may not consent to click-through agreements for the purposes of university business. If individuals approve these agreements, they would be personally responsible in any legal actions related to the services.

UC provides a variety of applications and services that support instructional, administrative and research activities by faculty, staff and students while meeting UC's policies, standards and guidelines. UC may have agreements with specific vendors or offer university-hosted solutions that meet your needs.

Challenges with Cloud Computing

Applications and services that are not purchased or licensed by UC, including those freely available on the Internet, such as popular social media sites, may not meet university standards for user privacy, security, intellectual property protection and records retention.

Potential problems with non-university approved applications include:

> Intellectual Property and Copyright - Terms of Service from many providers include provisions about who owns intellectual property rights when content is

created or uploaded to the application or service that may confuse intellectual property ownership claims. Cloud computing providers may reserve the right to change their Terms of Service at will.

Privacy and Data Security:

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/or security of that data are then potentially at risk. State and federal law mandate protection of sensitive information such as student data, social security numbers and credit card information. See the Data Governance & Classification Policy and the Acceptable Use of University Information Technology Resources Policy.

Data Availability, Accessibility and Records Retention:

UC is a public institution and, as such, is subject to public records law. In general, the Ohio Public Records Act requires that records that document the organization, functions, policies, decisions, operations or other activities of the university be made available to any member of the general public upon request, regardless of where they are stored.

However, many providers assume no responsibility for archiving content or ensuring availability, which places the burden on the user to ensure availability.

Additionally, UC is committed to ensuring that information, including any materials provided through internet applications and services, meet reasonable standards of accessibility for all.

UC also requires that instructional, administrative, and research records be retained according to the university's record retention schedule. See UC General Records Retention Schedule.

Cloud Computing Best Practices

Laptop and desktop computers, both university owned and non-university owned should install and run antivirus software. University owned computers accessing restricted data are required to run antivirus software. The university provides free antivirus for faculty, staff and students.

The University of Cincinnati believes that a strong awareness of information security issues is essential to all faculty, staff and students. Refer to the IT@UC Office of Information Security (OIS) Awareness web page for relevant information.

Intellectual Property and Copyright

- Remember that many UC images and symbols are owned by the university and not freely available for reproduction. Review and understand University Rules on Patents and Copyright, specifically, Patents and copyrights: Policy on inventions and discoveries (3361-10-19-01) and Patents and copyrights: Copyright policy (3361-10-19-02).
- Remember that students, except in a limited number of circumstances, own their work.
- Ensure that students understand appropriate use of copyrighted materials, particularly when content is publicly available.

Privacy and Data Security

- Never divulge information that the university has classified as "controlled or restricted" per the Data Governance & Classification Policy on the Internet. Examples include social security numbers, credit card information and driver's license numbers.
- Comply with FERPA requirements to protect student privacy. Do not place grades or evaluative comments on Internet sites. Contact the Office of the Registrar at 556-1000 for assistance interpreting FERPA. See University Rule Records: rights of privacy, general policy and procedure. (3361:10-43-11).
- Never use personally identifying information without explicit permission, unless the university has classified the information to be public, for example, in the University Directory.

Data Availability and Records Retention

- Ensure that all records, whether instructional, administrative or research are retained according to the records retention schedule. See the General Records Schedule for additional information.
- Ensure that applications or services are accessible to all. See UC's Web Policy for additional information.
- Back up materials regularly to ensure that records are available when needed, as many providers assume no responsibility for data-recovery of content.

Additional Tips

Tips for Instructors

- Communicate the issues, conditions and risks associated with any tool you choose at the beginning of the academic term, preferably in the syllabus.

This allows students who object to withdraw from the course or to request alternate assignments or other solutions. However, be sensitive to the fact that withdrawal may not be possible if the course is required, the course is offered in a sequence, the course is not offered regularly, or the course is only offered by one instructor.

- Restrict online access to student content as much as possible within the context of your instructional goals. In general, coursework conducted online should always be restricted to members of the course.
- Always require students to use aliases when creating accounts, particularly if access to student work is public. Also, prohibit use of the UC user name and password as an alias.
- Never include personally identifying information about yourself or your students in content or in profile information online.

Tips for Researchers

- Communicate the issues, conditions and risks associated with any tool you choose to use in the research process. This allows a potential participant who objects to withdraw from the study or to request alternate solutions.
- Always require participants to use aliases when creating accounts, particularly if access to research is public.
- Never include personally identifying information about yourself or your participants in online content or in profile information.
- Delete participant data when no longer required.

Tips for Administrators

- Clearly define organizational roles and responsibilities in creating a public presence for your unit.
- Remember that faculty, students and staff may not speak for the university.
- Set expectations with staff for online conduct.
  Manage your social media presence strategically and review it regularly.

Related links

Acceptable use of University Information Technology Resources Policy
Data Governance & Classification Policy
University Rules: Administration
General Records Schedule
Web Policy
Infrastructure, Platform and Software as a Service Policy

Phone Contacts

IT@UC Office of Information Security	513-558-ISEC(4732)	Infosec@uc.edu

History

Effective Date: 04/15/2015
Revised: 5/25/2017