# Information Security Policy
# Cloud Computing

| | |
|---|---|
| **Policy Name:** Cloud Computing | **Policy Number:** ISO PS023 |
| **Effective Date:** November 17, 2014 | **Review Date:** November 17, 2014 |
| **Last Revision Date:** February 3, 2015 | **Last Revision By:** Kim Adams |
| **Contact Name:** Kim Adams/Brenda Gombosky | **Contact Email:** ISOPol@louisville.edu |
| **Approved By:** Compliance Oversight Committee | **Version:** 1.1 |

## POLICY:

This policy applies to persons accessing and using any 3rd party service to transmit, store or share University sensitive (confidential or proprietary) data. Any such use must maintain the ability to protect the confidentiality, integrity and availability of the data in compliance with applicable regulations, laws and University policy.

## Purpose:

The purpose of this policy is to ensure that University sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing is a computing model that allows for easy, on-demand computing resources (networks, servers, storage, applications and services) that can be quickly provisioned and de-provisioned with minimal interaction and is accessible to users via the internet. Cloud computing can be defined as the utilization of servers or information technology hosting of any type that is not controlled by the University. Examples include: MicroSoft 365, Dropbox, Google Drive/Docs and third party email providers such as Gmail or Cardmail.

## STANDARDS:

### Administrative Standards

- **Implementation**
  The Dean of each School or Administrative Division Head is responsible for the promotion of these security policies and standards.

- **Documentation**

  - Procedures for complying with these policies and standards, as well as any additional school or division policies, standards and procedures will be developed and maintained by the designee for each school, division or other subsidiary unit.
  - All school or division policies, standards and procedures for computing devices should be well documented, up-to-date and meet the minimum requirements established in this policy and accompanying standards.

1 – See the Information Security Glossary for definition.

- **Compliance**
  - Each school or division is expected to ensure compliance with these policies and standards as well as their own policies, standards and procedures.

**Acquiring Cloud Computing Services**

The University of Louisville does contract with and use some cloud computing services. These services have strict contractual guidelines on use and protection of data. University faculty and staff must be very cautious about acquiring self-provisioned cloud services to process, store share or manage University data. Many of these services are free and users must agree to the terms of the providers EULA (End User License Agreement). The majority of these agreements state that there is no guarantee of protection of data stored, transferred or shared and do not allow for negotiation or clarification of terms. Cloud services may not meet federal, state or University compliance regulations and may be unvetted environments with significant risks. Users should review applicable data regulations and consult with the appropriate area within the university to ensure the data is allowed to be housed in a specified cloud environment.

- **Risk of Self-Provisioned Cloud Services**
  - **Security Risk**
    - **Data Breaches** – Unlike other computing services where contracts demand notification of data breaches – many cloud services do not and will not provide end user notification. Because of the 'shared' nature of these services, a flaw in one client's application can allow a hacker or malware to affect all other users of that service.
    - **Data Loss** – In addition to malicious activity, data loss can also occur due to mismanagement by the cloud provider such as the lack of proper backup and disaster recovery methods.
    - **Lack of Strong Authentication** – Without the proper safeguards and protection in place and up-to-date, your credentials can be compromised and used by others without your knowledge. This can allow access to not only your data but that of others using the service. Users should never use credentials in these environments that are used anywhere else, email, banking etc.

Individuals within the University community ***may not self-provision cloud services to store, process, share or manage University Sensitive (Confidential or Proprietary) data*** as defined by the Information Management and Classification Standard. If your division, school, department or office has a business need to acquire cloud services it must consult with the appropriate areas including IT, counsel, purchasing, information security and privacy to evaluate, manage risks and to ensure terms of service or contracts contain the required provisions. A request for review of cloud services can be submitted via the Information Security Policy Exception Form located at: http://louisville.edu/security/policies/policy-exception-process.

Use of cloud services for University Confidential or Proprietary information requires the approval of the data owner.

**Internal Resource Options**

If storage is required, secure enterprise servers is the recommended resource. Additional University resources are also available. Contact Enterprise IT if you have questions regarding the use of these resources.

University I: drive
Microsoft SharePoint
University Secure Email system
Large File Transfer process
Blackboard

**Technical and physical standards:**

- **Data Classification**
  - An important factor to consider when storing, transferring or sharing data outside the university is data classification. All data falls into one of the following classifications. Data with mixed classification should abide by the highest classification. It is important to note that some data requires the vendor to enter in to a third party agreement or business associate agreement in the area of HIPAA controlled data. Data users are responsible with complying with appropriate data use requirements. Refer to the *Information Management and Classification Standard* and the *Information Classification and Handling Guide* for additional guidance.
    - **Sensitive - Confidential –** Data whose unauthorized disclosure may result in a significant invasion of privacy, may expose the University to significant financial risk or result in negative impacts on the operations or reputation of the University. Data in any format collected, developed, maintained or managed by or on behalf of the university, or within the scope of university activities that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy. Examples include, but are not limited to regulations such as HIPAA, FERPA, PCI-DSS, HB-5 or personal data such as medical records (ePHI), social security numbers, credit card numbers, driver licenses, financial information, non-directory student records, and regulated research or export controlled technical data.
    - **Sensitive - Proprietary** - Data whose loss or unauthorized disclosure would cause adverse financial or reputational impact or lead to legal liability or otherwise impede the educational or business functions of the university. Examples include, but are not limited to, unclassified research work or protocols, strategy documents, draft documents prior to public release, financial information and information that would impair the security of the university physical or information environments.

- **Public** – Any data that does not fall in the other categories above, would be generally open to anyone without prior permission and would have no material adverse effect on the University community. Examples include but are not limited to advertisements, university catalogs, job postings, press releases.

## SCOPE / APPLICABILITY:

All persons while conducting/performing work, teaching, research or study activity or otherwise using university resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the university or affiliates.

## POLICY AUTHORITY / ENFORCEMENT:

The university's Information Security Office (ISO) in conjunction with Enterprise IT is responsible for the development, publication, modification and oversight of this policy and related standards. The ISO/IT work in conjunction with university leadership, Audit Services and others for development, monitoring and enforcement of the policy and standards.

## POLICY REVIEW:

This policy will be reviewed annually to determine if the policy addresses university risk exposure and is in compliance with the applicable security regulations and university direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed per the policy management process.

## COMPLIANCE:

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the university and/or action in accordance with local ordinances, state or federal laws.

## REVISION HISTORY:

| Version | Revision Date | Description |
|---|---|---|
| 1.0 | 11/17/2014 | Original Publication |
| 1.1 | 2/3/2015 | Addition of MS 365 to Cloud examples |

**This policy is subject to change or termination by the university at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

**Approved November 17, 2014 by the Compliance Oversight Council**
Shirley C Willihnganz, Executive Vice President and University Provost, Chair of the Compliance Oversight Council