Cloud Computing Services Policy and Guidance

Effective Date: 01/01/2016

Last Revised: 01/01/2016

Last Reviewed: 04/07/2017

Purpose

This Cloud Computing Policy and Guidance outline the practices and approval processes for using cloud computing services, platforms and infrastructure for the processing, exchange, storage or management of institutional data at The Moody Bible Institute of Chicago ("MBI").

Audience

All MBI employees

Background Information

Cloud computing services are application, platform, and infrastructure resources that users access via the Internet. These services, contractually provided by companies such as Apple, Google, Microsoft, Dropbox, Box.com, Amazon, and others enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide support for a wide range of business activities, such as communication; collaboration; project management; scheduling; and data analysis, processing, sharing, and storage. Cloud computing services are generally accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones), and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

Most cloud services, such as Google Docs, make it easy for individuals to sign-up and use (self-provision) their services via an end user license agreement (EULA), often at no monetary cost. MBI faculty, staff and other employees are prohibited from self-provisioning a cloud service to process, share, store, or otherwise manage MBI institutional data. Self-provisioned cloud services may present significant data management and compliance risks and may be subject to changes with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

Risks to Using Self-Provisioned Cloud Computing Services

Risks with using self-provisioned cloud services include:

- Unclear, and potentially poor access control or general security provisions
- No clear guarantee for service and availability

- Sudden loss of service without notification
- Sudden loss of data without notification
- Data stored, processed, or shared on cloud service is often mined for resale to third parties in a manner that may compromise people's privacy and be inconsistent with legal and regulatory requirements.
- The exclusive intellectual rights to the data stored, processed, or shared on a cloud service may become compromised.

In contrast to self-provisioned cloud services, MBI helps mitigate risks involved in using cloud services by negotiating agreements with cloud service providers for enterprise cloud services in a manner focused on compliance with legal, technical and security requirements in vetted environments where risks are better measured and evaluated by MBI.

Using Cloud Computing Services

Using a third party cloud service to handle institutional data does not absolve you from the responsibility of ensuring that the data is properly and securely managed. Members of the MBI community are expected to responsibly maintain and use institutional data regardless of the resource used to access or store the data—whether an institutional system, a privately owned resource, or a third-party resource.

The care taken to review a cloud services' security and trustworthiness must match the sensitivity of the institutional data you are looking to support with the service and the data's governing regulatory environment.

MBI POLICY AND PROCEDURE FOR PROCURING CLOUD COMPUTING SERVICES

In order to use a cloud service to store, process, share, or otherwise manage MBI institutional data, MBI employees, divisions, and departments must work with Information Technology Services and the Legal Department as specified below in order to properly evaluate and manage the risks that come with using the service for institutional data.

• Consult with Information Technology Services. To begin this process please submit a service ticket to the ITS Service Desk at ITS@moody.edu or call X4067. Information Technology Services will guide the requestor through the Guidance Process below.

• Review the framework below for classifying institutional data and, in consultation with Information Technology Services and the Legal Department to determine the classification framework applicable to the institutional data that will be placed into the cloud service.

Confidentiality Level	**Description**
Level A: Regulated Institutional Data	Regulated institutional data is data that is regulated by information privacy or protection laws, regulations, contracts,

	binding agreements (such as non-disclosure), or industry requirements.
Level B: Confidential Institutional Data	Institutional data that is meant for a very limited distribution— available only to members of the MBI community on a strictly need-to-know basis.
Level C: Administrative Institutional Data	Institutional data that is meant for a limited distribution; available only to members of the MBI community that need the institutional data to support their work. This institutional data derives its value for MBI in part from not being publically disclosed.
Level D: Public Institutional Data	Institutional data that is meant for members of the MBI community and in some cases wide and open distribution to the public at large. This institutional data does not contain confidential information.

- Review Guidance Process section below and work with Information Technology Services to conduct due diligence on the cloud provider and cloud services and with the Legal Department to develop the appropriate contractual safeguards.
- Monitor changes to the cloud service.
- Have a clearly designated Information Manager for the institutional data. The Information Manager is the individual charged to ensure the responsible management and use of institutional data.
- Use of cloud computing services must comply with all current laws, ITS security and risk management policies, including, without limitation, all applicable privacy laws and regulations. Appropriate language must be included in the contract or vehicle defining the cloud computing source responsibilities for maintaining privacy.
- In addition to the VP of ITS, the VP of the department requesting use of the cloud service, sufficiently familiar with the context of the use of the service and adequately informed of the associated risk through a documented risk assessment, must document an acceptance of risk and provide written authorization of the use of the service.
- For external cloud computing services that require users to agree to online terms of service agreements, such agreements must be reviewed by both ITS and the Legal Department, and approved as to legal form, prior to accepting such terms of service.
- **All use of cloud computing services must be approved in writing by the VP of ITS and the Legal Department following verification that security, privacy and other IT management and contractual requirements have been adequately addressed prior to use of any cloud computing services.**

- Know and adhere to any legally mandated and MBI required retention period and, when applicable, ensure timely and secure destruction of the institutional data as may be required by law or MBI policy. Retention periods may be found in MBI's general Data Retention Policy or other records policies.

Guidance Process

Many issues should be considered carefully before adopting a cloud computing solution. The list below features some of the more important issues Information Technology Services will help you to consider, and to address in contract language when appropriate:

• Determine why the Department needs to use a cloud computing approach. What are the drivers? Several possible drivers are listed below.

  • More efficiency or effectiveness for the IT investment.

  • Need for a specific cloud computing characteristic (elasticity, scalability, usage-based model).

  • Need for rapid implementation

• Be realistic in cost estimates. Consider the total lifecycle costs, not just the cost of implementation.

• Acquisition strategy

  • Identify and consider appropriate existing contracts and cloud computing solutions already in use at Moody before acquiring new services.

  • When acquiring new services, consider how services can be architected and agreements written in a way that would enable broader use/adoption of the service across Moody.

• ITS security

  • Match ITS security requirements and the security capabilities of the cloud computing implementation to those of the mission/business needs being supported.

  • Weigh the security threats and opportunities that are present for public, private, and community Clouds

  • Consider how issues of logging, incident reporting, response, forensics, and other security-related functions should be addressed with respect to the cloud computing service provider.

  • Consider how disaster recovery and continuity of operations planning will be addressed.

• Privacy impact

  • If Personally Identifiable Information (PII) or other sensitive information is involved, document how it will be protected and who is allowed access to it.

    - If the cloud computing source is keeping user usage statistics, consider the privacy implications involved and define appropriate safeguards to assure user privacy is maintained. This would include session logs and security access logs, among others.

- Records Management
    - Identify all systems of records to be hosted in the cloud.
    - Identify the schedules for all records and include the information on retention as part of the agreement with the vendor.
    - Specify the retention time for all system backups.
    - Consider how records management and electronic discovery will be managed in the cloud environment.
- Consider implications of using a service model that is different from the traditional use of Moody-owned and -operated infrastructure.
- Identify which issues should be explicitly documented in service level agreements.
- Consider issues of interoperability with existing systems.
- Consider issues of data ownership and portability. How would you migrate from a given Cloud Computing infrastructure to another one at some point in the future?
- Examine the need for additional training for Departmental staff.
- Focus on the requirement driving the need, not the technology used to implement it.
- Determine how mature the industry offerings are for the implementation under consideration.

Contacts

If you have questions or concerns about this policy, please contact the Information Technology Services Support Center at 312.329.4067 or ITS@moody.edu for assistance.

If you have questions about the policy, you may email ITSpolicy@moody.edu for assistance.