MOODY BIBLE INSTITUTE

Remote Data Storage and File Sharing

Effective Date: 05/1/2017
Last Revised: 04/13/2017
Last Reviewed: 04/13/2017

Scope

This policy applies to all employees and persons accessing Moody Bible Institute's (MBI) data via onsite or offsite means. The VP of Information Technology Services must approve exceptions to this Policy.

Purpose

The purpose of this policy is to ensure that MBI data is not inappropriately shared or stored using public cloud computing and/or file share services. For the intent of this policy, cloud computing and file sharing is defined as the use of servers or information technology that is not controlled by or associated with MBI. A list of all acceptable services is listed in the section titled Approved Services of this policy.

Reason for Policy

This policy endorses the use of the Dropbox Education cloud service for file storing and sharing 1) with vendors who can provide appropriate levels of protection and recovery for MBI information, and 2) with explicit restrictions on storage of MBI Protected Information. While cloud storage of files can expedite collaboration and sharing of information anytime, anywhere, and with anyone, some guidelines need to be in place for MBI information that is appropriate for storing and sharing using Dropbox Education.

There are a number of information security and data privacy concerns about use of cloud computing services at MBI. They include:

- MBI no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws.
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- MBI dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor

MBI is reliant on vendor's services for the security of some academic and administrative computing infrastructure

Policy

The following table outlines the data classification and proper handling of MBI data.

Data Classification	**Cloud Storage (See approved services for list)**	**Network Drive** ***(ID and Password Required)***	**Local Storage**
Protected	**Not Allowed**	**Allowed** No special requirements, subject to any applicable laws	**Not Allowed**
Sensitive	**Allowed But Not Advised** Requires Dept. Manager approval	**Allowed** No special requirements, subject to any applicable laws	**Allowed But Not Advised** Requires Dept. Manager approval
Public	**Allowed** No special requirements	**Allowed** No special requirements	**Allowed** No special requirements

Protected Data—any data that contains personally identifiable information (PII) personal health information (PHI) concerning any individual and is regulated by local, state, or Federal privacy regulations.

Sensitive Data—any data that is not classified as Protected Data, but which is information that MBI would not distribute to the general public. Ex. Salary history, performance improvement plans, confidentially shared information, etc.

Public Data—any data that MBI is comfortable distributing to the general public.

Use of MBI servers, where authentication is required, is the best place to store all categories of MBI data, particularly MBI Protected data. It is never acceptable to store MBI Protected data on any cloud service. This includes data that would be classified as HIPPA, FERPA, PII, PCI, and PHI among others.

The following restrictions apply to the sharing of MBI data. Where there is a requirement to share information with others then it is important that individuals who enable the sharing of data do so with the following safeguards:

- Grant access to the specific folders and files that are required to support the collaboration or information sharing and ensure that no other folders or files are made available.
- Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honor all security requirements as well as privacy or confidentiality commitments.
- Delete data from shared folder when no longer needed.

Synchronizing information to and from Allowable Cloud Storage can provide significant advantages in terms of information availability and speed of access. Synchronizing information across a range of devices requires the following safeguards:

- Individuals must ensure that the devices involved in the synchronization process are protected as far as possible from unauthorized access or loss. Mobile devices must have a “PIN” code or equivalent enabled.

  Individuals must ensure that the devices involved in the synchronization process are protected as far as possible from malware and are kept up to date with vendor supplied security patches.

Compliance Data

MBI has many federal laws that it must follow, among those include the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA).

State laws may also affect a relationship with a cloud-computing vendor. For instance, the Illinois Personal Information Protection Act (IPIPA) requires that the MBI must follow rules about disclosing Social Security Numbers as well as specific security breach notification procedures.

Note: A relationship with a cloud-computing vendor may also be impacted by private industry regulations. For example, departments at MBI that accept credit cards also must follow the Payment Card Industry (PCI) Data Security Standard (DSS) issued by the major credit card companies.

Any Institute data will not be stored, shared, or otherwise processed by any non-Institute owned equipment, network or service unless the organization enters into a legally binding agreement with Moody to protect and manage the data according to standards and procedures acceptable to the Information Technology Services department.

Finally, cloud-computing services that use, store, or process MBI data must also follow applicable MBI policies. Such policies may include Information Technology Services policies and MBI's data handling and retention requirements.

Definitions

There are numerous types of cloud computing services available on the Internet that may be appropriate for personal use, though they may not meet the security and confidentiality standards required for official Institute use. Some examples are:

- *External Email Services* (e.g., Hotmail, Gmail, Yahoo Mail, etc.)
- *Chat & Instant Messaging Services* (e.g., Yahoo, AIM, MSN, IRC, Twitter, etc.)
- *Social Networking Services* (e.g., MySpace, Facebook, YouTube, Friendster, etc.)
- *Hosted Application Services* (e.g., Google Apps for Education, Amazon Web Services, etc.)
- *Peer to Peer File Sharing* (e.g., Kazaa, Gnutella, Bit Torrent, LimeWire, Morpheus, etc.)
- *Virtual Machines* (e.g., GoGrid and Amazon Elastic Compute Cloud are commercial web services that allow customers to rent any number of virtual computers upon which they can load and run their own software applications.)

Approved Services

Because of privacy and security concerns, only approved services may be used for cloud storage and file sharing. This list may be revised and notifications of such revisions will be published here as well as notification done electronically via email or the ITS website. Currently only MBI’s corporate Dropbox Education can be used.

Should you ever need to store or share Moody data in a manner not currently provided within the Institute’s secure computing environment, please contact the ITS Support Center and we will work with you to identify and attempt to provide a solution that best protects Moody’s data.

Policy Adherence

Failure to follow this policy can result in disciplinary action as provided in the Employee Information Guide. Disciplinary action for not following this policy may implemented up to and including termination from employment.

Contacts

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

Related

Data Retention Policy, PCI 3.1 and Inventory Asset Policy

Appendix

Data that is stored or transmitted electronically is considered protected if their unauthorized release can result in harm to the institution or to individuals. Such harm may include identity theft, legal or financial liability, institutional or personal embarrassment, as well as other consequences. It is the responsibility of all employees of MBI and others who are empowered to act on behalf of the Institute to protect confidential data from unauthorized access and/or misuse.

The following guidelines are intended to help you identify data items that should be treated as protected. However, the lists below are not exhaustive and there are protected data items that fall outside of these guidelines. If you are uncertain about the status of a particular data item, please consult with your supervisor or reach out to the ITS Support Center.

Identity Theft Material

Identity theft is the fraudulent use of another's personal information for financial gain or to perpetrate other illicit activity. Unauthorized access to materials that can be used for identity theft can expose individuals to harm and, in certain cases, expose the institution to financial liability, public relations challenges, and other types of problems. This applies to all employees, students, alumni, donors, parents, board members, vendors, and others –– whether they are current, former, or prospective –– whose personal data is electronically stored or transmitted by the Institute. In conjunction with an individual's name, data related to identity theft include:

- Date of birth
- Social Security Number
- Driver's license/passport/ID numbers
- Credit card numbers, expiration dates, PINs
- Account numbers (banks, brokerages, utilities, etc.)
- Passwords for accounts, databases, and other resources

These items can be found in documents such as tax returns, admissions applications, credit, loan and other types of applications, housing agreements, employment records, student records, financial correspondence, etc.

Employee Information

In addition to material that can be used in identity theft, other personal data items that are to be treated as sensitive include:

- Compensation and promotion information
- Benefits information
- Performance reviews, disciplinary materials, and related documents
- Worker's compensation, disability claims, or other medical information

Donor Information

Details about donors should be treated as protected data including:

- Information on records marked confidential
- Activities/events attended
- Children/family information
- Contact reports
- Correspondence history
- Gift/Pledge data

Student Information

The Family Educational Rights and Privacy Act, FERPA, gives students four specific rights:

- to see the records that the institution is keeping on the student;
- to seek amendment to those records and in certain cases to append a statement to a record;
- to consent to disclosure of his/her records;
- to file a complaint with the FERPA Office in Washington.

All of this information would fall under a protected classification.

Under FERPA the following data items may be not be disclosed unless appropriately authorized:

- Grades
- Financial aid information
- Credit Card Numbers
- Bank Account Numbers
- Wire Transfer information
- Payment History
- Student Tuition Bills

In addition, students have the right to restrict disclosure of the following items:

- Name
- Date of birth
- Place of birth
- Campus address and phone number
- Campus mailbox number
- Electronic mail address
- Permanent mailing address
- Permanent phone number
- Secondary mailing address
- Semesters of registration at Reed
- Full or part-time status
- Reed major, degree(s) awarded and date(s)
- Institution attended prior to Reed
- Honors awarded
- Participation in Reed College programs
- ID card photographs

Under Health Insurance Portability and Accountability Act, HIPAA, the following data may not be disclosed unless appropriately authorized and is classified as protected data:

- Patient Name
- Street address, city, county, zip codeBirth date (except year)
- Location or dates of treatment
- Contact information: phone, fax, email, etc.
- Social security number
- Account/Medical record numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle ID's & serial numbers
- Device ID's & serial numbers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment guarantor's information

Other Information

Other data items whose unauthorized use could directly or indirectly harm the institution or individuals should be classified as sensitive and include:

- Class rosters
- Academic records and notes
- Human subject data
- Materials related to internal or external investigations
- Legal documents and records
- Financial records, grants, and contracts
- Campus security plans and procedures
- Storage sites for confidential data
- Email containing sensitive information
- Meetings minutes, memos, notes, emails, and other materials related to sensitive topics such as personnel matters, student behavior, etc.