Information Security Policy

Effective Date: 03/01/2009
Last Revised: 07/20/2015
Last Reviewed: 04/15/2016

Audience

All users of the Moody Bible Institute network and computer systems

Policy

The information assets of Moody Bible Institute (MBI) must be available to the MBI community, protected commensurate with their value, and must be administered in conformance with federal and state law. Reasonable measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to reasonably assure the confidentiality, integrity, availability, authenticity of information. Reasonable measures shall also be taken to reasonably assure availability, integrity, and utility of information systems and the supporting infrastructure, in order to protect the productivity of members of the MBI community, in pursuit of the MBI mission.

Therefore, MBI will take reasonable steps to:

Assign a staff person to the position of Information Security Administrator whose duties and responsibilities are to develop and manage Information Technology Services security polices including disaster recovery, data security, and application security. Act as consultant and advisor to other areas on security and risk evaluations. This position will update policies and procedures annually in accordance with PCI and financial institution requirements. *See HR Information Security Administrator Job Description*

Develop, publish, maintain, and enforce standards and policies for lifecycle protection of MBI information systems and supporting infrastructure in the areas of networking, computing, storage, human or device/application authentication, human or device/application access control, incident response, applications or information portals, electronic messaging, and encryption. *See ITS Policies and Procedures posted on Portal*.

Provide training to authorized Institute users in the responsible use of information, applications, information systems, networks, and computing devices. *See MBI Computer Use Policy and User Account Access Policy & Procedure*

Develop, publish, maintain and enforce standards to guide MBI business associates and outsource partners in meeting MBI's standards of lifecycle protection when handling MBI information or supporting MBI information systems and supporting infrastructure. An internal and external scan will be conducted quarterly by an outside approved vendor. ITS will have a penetration test performed annually in accordance with PCI standards and performed by an outside certified QSA vendor.

Encourage the exchange of information security knowledge, including threats, risks, countermeasures, controls, and best practices both within and outside the Institute. *See Enterprise Applications Best Coding Practices*

Check and review security logs daily to minimize exposures of potential breaches. Review all critical system components (for example, firewalls, and intrusion detection systems / intrusion prevention systems), authentication and e-commerce redirection servers periodically in accordance with risk assessment strategies. Examine documentation and interview personnel that ITS security policies and operational procedures are being followed. Follow up exceptions and anomies identified during the review process. *See Track and Monitor Policy*

Periodically evaluate the effectiveness of information security controls in technology and process. All non-leased devices holding cardholder data shall be tagged with owner, contact information and purposes. Establish and maintain information classifications, protection and destruction protocols through multiple policies and procedures. *See Information Retention at Departure of Employment Policy, Data Retention Policy and Credit Card Data Retention & Disposal Policy*

Establishment and maintenance of a policy and procedure regarding confidentially agreements for every staff, vendor and student employees. *See ITS Confidentiality and Security Policy and Password Policy*

Establish and maintenance of institute networks, systems, assets and applications use with appropriate levels of protection. *See Cloud Computing Services Policy and Guidance, and Inventory Assets Policy*

Establish and maintain polices regarding Internet, email usage and acceptable use policies, along with keeping the community aware of guidelines and acceptable practices. *See MBI Computer Use Policy, Email Policy, Clear Screen Policy and Desktop Computer Security Policy*

Designate one or more individuals to identify and assess the risks to non-public or business-critical information within the Institute and establish an Institute-wide information security awareness program with regular alerts and notifications.

Definitions

Information Safeguards: Administrative, technical, and physical controls that support the confidentiality, integrity, availability, and authenticity of information. *See Enterprise Applications Best Coding Practices*

Information systems and supporting infrastructure: Information in its analog and digital forms and the software, network, computers, tokens, and storage devices that support the use of information. *See Computer Room Access Policy*, *Multi-Function Devices/Printers, Bring Your Own Device (BYOD) Policy and Select Your Own Device*

Lifecycle Protection: Information systems and supporting infrastructure have a lifecycle that begins with evaluation and selection, and advances through planning, development/ acquisition, and operations through to disposal or retirement. Information safeguards are needed at all phases of the lifecycle. Controls depend on the system, its capabilities, and expected usage, as well as anticipated threats against the information *See Employee Departure Policy*

Preventive controls include use of encryption, information integrity measures, security configuration, media reuse, use of antivirus, and physical protection. *See Network Configuration Policy and Firewall / Router Review Policy*

Detective controls include network and information access monitoring, and intrusion detection (host based or network based), manual or automated review of security logs. *See Track and Monitor Policy*

Corrective controls include recovery plans for handling isolated information safeguard failure incidents to business continuity plans. *See Computer System Backup Policy*

Procedures / Documents

See PCI DSS 8.5.14 / 10.6.1, 2, 3 / 11.6
See HR Information Security Administrator Job Description
See MBI Computer Use Policy
See User Account Access Policy & Procedure
See Internal and External Scan Policy
See Track and Monitor Policy
See Enterprise Applications Best Coding Practices
See Information Retention at Departure of Employment Policy
See Data Retention Policy
See Credit Card Data Retention & Disposal Policy
See ITS Confidentiality and Security Policy
See Password Policy
See Cloud Computing Services Policy and Guidance
See Inventory Assets Policy
See Email Policy
See Clear Screen Policy
See Desktop Computer Security Policy
See Computer Room Access Policy
See Multi-Function Devices/Printers
See Bring Your Own Device (BYOD) Policy
See Select Your Own Device
See Employee Departure Policy
See Network Configuration Policy
See Firewall / Router Review Policy
See Computer System Backup Policy

Contacts

If you have questions or concerns about the execution of this policy, you may 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.

Related

- n/a