University of Maryland Baltimore (UMB)
Center for Information Technology Services (CITS)

IT Security Program

Purpose

This document provides direction for managing and protecting the confidentiality, integrity, and availability of UMB information assets. The purpose of the IT Security Program is to:

- Document the roles and responsibilities for the information security program
- Assess risk and establish mitigation strategies
- Define security-related policies and procedures
- Conduct compliance reviews
- Establish a security awareness and training program
- Monitor the security program's effectiveness

Scope

Consistent with UMB security policies, the IT Security Program shall apply to the following:

- Centrally and departmentally-managed University information assets.
- All users employed by the University, contractors, vendors, or any other person with access to the University's network resources or information assets. This includes non-UMB-owned computing devices that may store protected information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).
- Information technology facilities, applications, hardware systems, network resources owned or managed by the University. This includes third party service providers' systems that access or store the University's protected information.

Auxiliary organizations, external businesses and organizations that use University information assets must operate those assets in conformity with the University's IT Security Program.

Roles and Responsibilities

The Information Security Officer oversees the IT Security and Compliance Office and is responsible for the overall management, implementation, and enforcement of the IT Security Program. The Information Security Officer reports directly to the Chief Information Officer/Vice President (CIO/VP) of the University.

The overall responsibilities of the IT Security and Compliance Office are to:

- Coordinate, administer, communicate, and maintain the IT Security Program.
- Advise the CIO/VP and University leadership on information security matters.
- Consult with University administrators to ensure information security policies meet University goals.
- Confer with CIO/VP and IT leaders on information security policies, procedures, campus security risks and other security matters as needed.
- Respond to information security related requests during an audit and coordinate the University's information security audits.
- Manage the disaster recovery plan and coordinate bi-annual updates and annual testing activities.
- Serve as the Center for Information Technology Services' (CITS) point of contact for the University's Continuity of Operations Plan (COOP).
- Develop and implement internal controls, policies and procedures to assure compliance with University policies as well as applicable state and federal regulations and guidelines.
- Manage all applicable audits, such as legislative audits, University System of Maryland (USM) audits, and other relevant audit activities.
- Act as an independent review and evaluation body to ensure compliance.
- Coordinate the annual review of the University IT and CITS internal policies, plans and procedures.
- Serve as the University representative on identified security committees.
- Review justifications for access to sensitive information or variance from a standard operating procedure.
- Oversee the University incident response program, the information security awareness and training program, and annual assessment review of the security program.
- Review information security incident reports and determine action needed.

Security-related Policies, Plans, and Procedures

UMB's IT Security Program, combined with the IT Acceptable Use Policy, establishes policy and sets expectations for protecting University information assets. These are supported by related policies, plans and procedures to facilitate University compliance.

The IT Security and Compliance Office is responsible for coordinating the development and dissemination of information security policies, plans and procedures. Approved policies, plans, and procedures will be published on the web, incorporated into security training programs, and disseminated through available University communication methods. They will be reviewed annually to determine if any changes are required.

The University information technology security-related documents can be found on the CITS web page at: http://www.umaryland.edu/umbcomputingpolicies/

Compliance Reviews

UMB's information security practices must comply with a variety of state/federal regulations and University policies/procedures. The reviews conducted for the University will be administered on an annual basis and will comply with:

- University security policies and procedures
- USM IT Security Standards
- External and internal IT audit findings (e.g., legislative audits, University System of Maryland audits, disaster recovery audits)

Security Awareness and Training

The IT Security Awareness and Training program is designed to help individuals protect and respond appropriately to threats to University information assets. The program promotes awareness of:

- UMB information security policies, plans and procedures
- Potential threats against University protected data and information assets
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets
- University notification procedures in the event protected data is compromised

Listed below are the methods used to provide security awareness and training.

- KnowBe4 Security Awareness Training - UMB has contracted with KnowBe4 to provide interactive web-based security awareness training. This customized program consists of targeted training modules which can be accessed via UMB's Learning Management System (LMS).
- Information Security Web Page - The information security web page can be accessed by all University employees and will provide access to campus security-related policies and procedures. General security Dos and Don'ts as well as a monthly Tips and Tricks will be included.
- Campus IT Security Meetings - Monthly meetings will be held with the IT security contacts for all schools and departments. This will provide an opportunity to share security-related information and address questions from the campus community.

- Center for Information Technology Services (CITS) Internal Security Meetings - Weekly meetings will be held with internal CITS staff. These meetings will be used to share security-related information as well as to address security-related audit issues.
- Monthly Security Communication - A free monthly security newsletter, "OUCH," will be emailed to all University security personnel to be shared with their users. "OUCH" is the world's leading, free security awareness newsletter designed for the common computer user. Each edition is carefully researched and developed by the SANS subject matter experts and team members of the community.

Program Evaluation

Monitoring the effectiveness of the security program can be challenging, but plays an important role in protecting the confidentiality, integrity, and availability of critical information assets. The goal of the evaluation is to assist the University in:

- Building a robust information security program
- Preparing for future reporting and audit requirements
- Responding to audit findings
- Improving overall security posture

UMB assesses the effectiveness of its IT Security Program by completing the annual IT Security Program Status Report conducted by the University System of Maryland (USM). This report is used to evaluate and enhance the effectiveness of the program.

Related Security Information

- Maryland Department of Information Technology Information Security Policy – This policy describes security requirements that Executive Departments and Independent State agencies must meet in order to protect the confidentiality, integrity, and availability of state owned information.
- USM IT Security Standards, Version 3.0, June 2014 – This document addresses security standards established by the Department of Information Technology (DoIT) for state agencies and interprets those standards in the context of the University of System (USM) institutions.
- Higher Education Information Security Council (HEISC) – The Higher Education Information Security Council mission is to improve information security, data protection, and privacy programs across the higher education. HEISC actively develops and promotes leadership; awareness and understanding; effective practices and policies; and solutions for the protection of critical data, IT assets, and infrastructures. http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/about

Risk Assessment and Mitigation

Information security risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk to information security assets.

Risk management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk. A risk management policy is critical for UMB to successfully implement and maintain an acceptable level of information security. Once a risk has been identified, mitigation strategies are developed to reduce the risk to acceptable levels or assume the identified risk. Risk management should not only engage changes to existing systems, but should also integrate into the life cycle for new systems.

Risk identification is the first phase of risk management and should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences.

Risk assessment is the second phase of risk management and is used to determine the extent of a potential threat and the risk associated with it. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk mitigation, the third phase of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Risk evaluation is the fourth phase and is ongoing and evolving. Evaluation assists in developing an effective risk management program within the IT security program.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. To assess risk, critical assets must first be identified. An analysis is then performed to determine the types of threats that may exist against the asset; the level of vulnerability of the threat must also be determined. Not only should the risk management program engage changes to existing systems, but should also integrate into the life cycle for new systems.

The following sequence of activities will be used in performing an information security risk assessment as well as conducting pre-implementation control reviews for new systems:

1. Identify critical assets in central units, starting with departments that manage student, financial and human resources data, and collaborating with the IT leaders in schools and departments to undertake an assessment in those areas.

2. Assess risk by applying the UMB data classification category for each asset/organization
    - Level 0 – Public - Non-critical data (i.e., public directory information). Data explicitly or implicitly approved for distribution to the public where there is little institutional risk associated with this system due to security.

- Level 1 – Internal - Data intended for internal University use. Applications or services that support academic instruction, research data or general communications that do not contain sensitive information.
- Level 2 – Confidential - Critical data, systems, applications or services related to or supporting the commitment or management of UMB financials, student data, research and those systems containing sensitive information (i.e., name, SSN or other combination or personal identifiers) which if compromised could be used to commit identity theft.
- Level 3 – Regulated - Highest risk data, systems and applications or services that have externally mandated IT compliance requirements such as those containing information covered by HIPAA (Health Insurance Portability and Accountability Act) or PCI (Payment Card Industry). Failure to comply with these externally mandated IT security requirements may result in serious financial, legal and/or reputational harm to individuals and/or the University.

3. Implement a default risk mitigation strategy in order to strengthen the security for all University owned systems with additional consideration for those systems that have access to sensitive data in the Student, HR and Financial systems the following controls will be required to be implemented.
    - Identify everyone with access to sensitive data in our central systems, student, HR and Finance and make sure that they have the IdentityFinder client installed and monitored.
    - Implement whole disk encryption for University owned workstations and laptops.
    - Implement application whitelisting.
    - Remove administrative rights for all users.

4. Evaluate on a periodic basis the security status of all campus assets with regards to patching, antivirus and adherence to default risk mitigation actions.