**College/School Name: Katz School**

**Department/Program Name: MS in Cybersecurity**

**I.          Department/Program Mission Statement**

The mission of the Master’s in Cybersecurity is to prepare students for employment in various cybersecurity-related fields by ensuring the students are exposed to the many different disciplines and technologies required to protect organizations and governments and other critical infrastructures.

**II. Department/Program Student Learning Goals**

Graduates will leave the MS in Cybersecurity with a demonstrable ability to:

1. Identify and articulate organizational cybersecurity risks.
2. Establish, manage and evaluate an organization’s cybersecurity foundation.
3. Develop an effective internal and/or external communication strategy.

**III. Department/Program Student Learning Objectives:**

|  |  |
| --- | --- |
| **Department/Program Goal** | **Objectives** |
| Identify and articulate organizational cybersecurity risks. | Explain current standards and practices in cybersecurity and how they are applied  to cyber exposures and threats, including systems design, methods, and techniques aimed at prevention, mitigation, response, and recovery from cyber-attacks and intrusions |
| Develop a risk based approach to managing operational factors associated with cybersecurity. |
| Establish, manage and evaluate an organization’s cybersecurity foundation. | Explain operating system security architecture concepts, including integrity and access control based security models and design, kernel protection, trusted  platform module, and security auditing. |
| Discuss the importance of operating system, embedded system and application testing for errors, and vulnerability and defect testing methodologies |
| Develop an effective internal and/or external communication strategy. | Assess the importance of real-time internal hardware and software intelligence and the steps an organization must take to develop a comprehensive risk management strategy and policy. |
| Apply communication techniques to inform management of the need for IT Risk Assessment and Management procedures. Apply communication techniques to inform management of the need for IT Risk Assessment and Management procedures. |

**IV. Curriculum Mapping**

**Definition:** Aligning courses with department and program level goals and objectives

**Directions:** Complete the table[[1]](#footnote-1) below by listing each learning objective/outcome for students in your department/program in the rows in the far left column. List the required courses/experiences in the remaining columns of the first row. Place an X in the cells of each course that targets each objective/outcome. A completed example by a psychology department is provided on the next page.

Levels Curriculum Map

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Learning objectives/outcomes   |  | | --- | |  | |  | | Required Courses/Experiences | | | | | | | | | | |
| **Cybersecurity Foundations** | **Architecture of Secure Operating Systems, Applications, and Devices** | **Risk Management and Cybersecurity** | **Cybersecurity Audit, Assessment, and Training (Cloud Security)** | **Leading Technology Organizations** | **E-Discovery, Digital Evidence, and Computer Forensics** | **Cybercrime, Cyberwar, and Threat Actors** | **Emerging Cybersecurity Threats** | **Internship** | **Capstone** |
| a. Explain current standards and practices in cybersecurity and how they are applied to cyber exposures and threats, including systems design, methods, and techniques  aimed at prevention, mitigation, response, and recovery from cyber-attacks and intrusions. | X | X | X | X | X |  |  | X | X | X |
| b. Develop a risk based approach to managing operational factors associated with cybersecurity. | X | X | X | X | X |  |  | X | X | X |
| a. Explain operating system security architecture concepts, including integrity and access control based security models and design, kernel protection, trusted  platform module, and security auditing.. | X | X | X | X |  | X | X | X | X | X |
| b. Discuss the importance of operating system, embedded system and application testing for errors, and vulnerability and defect testing methodologies. | X | X | X | X |  | X | X | X | X | X |
| a. Assess the importance of real-time internal hardware and software intelligence and the steps an organization must take to develop a comprehensive risk management strategy and policy. | X | X | X | X |  | X | X | X | X | X |
| b. Apply communication techniques to inform management of the need for IT Risk Assessment and Management procedures. | X |  | X | X | X | X | X | X | X | X |

1. Table adapted from Curriculum Mapping Template from Lehman College Office of Assessment and Planning. Retrieved Nov. 7., 2013 from http://www.lehman.edu/research/assessment/templates.php [↑](#footnote-ref-1)