UNIVERSITY OF DETROIT MERCY

Annual Assessment Report for Academic Programs

The University Assessment Team advocates for the enhancement of student learning through purposeful, meaningful, and feasible student-outcomes assessment practices. The Assessment Team seeks to collaborate with programs, departments, and units to ensure that effective assessment of student learning occurs across the University. To assist in meeting this goal, the Team requests that you complete this Annual Assessment Report form to document student learning in your program. A PDF version of this completed form will be posted to the Academic Affairs Assessment website. Please note that this Annual Assessment Report form should only be completed after you have an Assessment Plan for Academic Programs forms on file with the University Assessment Team. The plan is completed once and only updated when revisions have been made to components of the plan.

1. Degree Level and Program Name: BS in Cybersecurity

2. College/School: College of Humanities, Arts & Social Sciences

3. Assessment Overview - Briefly share how student learning outcomes assessment is conducted within your program/department (e.g. number of outcomes, examples of assignments used, and frequency of assessment).

The BS in Cybersecurity program has four student learning outcomes, with two outcomes assessed each year. Faculty assess student learning outcomes using direct measures from embedded assignments (e.g. hands-on technical labs, exams, design cases, and projects using rubrics).

4. Student Learning Outcomes -Which student learning outcome(s) from the assessment plan filed with the University Assessment Team is/are being reported on in this report? Include the corresponding benchmark(s) for each outcome.

Two student learning outcomes are being assessed in this cycle: Student Learning Outcome #1: Analyze a problem and identify and define the security risks and requirements appropriate to its solution. Students will successfully complete hands-on Lab: APPSERVER1 was compromised, and a summary of the incident was provided. Students must address four questions pertinent to the investigation.

Student Learning Outcome #2: Demonstrate the use of techniques, skills, and tools necessary for cyber defense within an organization. Students will download and install Wireshark and its required components, download and unzip Wireshark captures and successfully complete hands-on lab.

The benchmark for success is to have at least 75% of the students earn a rubric equivalent total score of C or better on the hands-on lab assignments.

5. Institutional Outcomes - For which institutional outcome(s) do the reported student learning outcome(s) align?

SLO Outcome Alignment	Institutional Outcome
Yes	I. Jesuit & Mercy Values
	II. Diversity & Cultural Awareness
Yes	III. Critical Thinking & Problem Solving
	IV. Communication
Yes	V. Professionalism
	VI. Lifelong Learning

6. **Assessment Period:** Select the academic year for which you are reporting results (i.e. when data were collected):

2023-2024

7. **Results, Planned Actions, and/or Actions Taken** -Briefly summarize the assessment results, how they relate to benchmark(s), and how you are using them to enhance student learning and improve program quality.

Outcome #1: 83% (10/12) of the CIS 3850, Cybersecurity Risk Management students earned a rubric equivalent score of C or better on the hands-on design case, which is above the 80% benchmark for the group of students. The aggregate mean rubric scores (using a 4-point scale) indicated students' strengths were in Identification of cybersecurity risk to the organization (3.33) and Respond-taking action regarding a detected cybersecurity incident (3.21). Students' opportunities for improvement were in Detecting all of the critical pieces of information (3.04).

Outcome #2: 80% (8/10) of the CIS 4450 Introduction to Digital Forensic students earned a rubric equivalent score of C or better on the Network Traffic Analysis With Wireshark hands-on lab, which is at the 80% benchmark for the group of students. The aggregate mean rubric scores (using a 3.5-point scale) indicated students' strengths were in downloading and installing a cybersecurity network scanning tool (2.75) and interpreting Wireshark packets, queries, and pcap information (2.6). Areas for opportunities for improvement include interpreting more in-depth packet scanning information (2.55).

Responding the results of both outcomes, the department reviewed and revised instructional materials and assignments to improve student competencies in the identified areas.

Attachment(s):

None