SAINT LOUIS UNIVERSITY.

Program-Level Assessment: Annual Report

Program: Cyber Security	Department: Online
Degree or Certificate Level: Graduate	College/School: School of Professional Studies
Date (Month/Year): 6/2020	Primary Assessment Contact: Dustin Loeffler
In what year was the data upon which this report is based collected? 2019-2020	
In what year was the program's assessment plan most recently reviewed/updated? 2019	

1. Student Learning Outcomes

Which of the program's student learning outcomes were assessed in this annual assessment cycle?

1. Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.
2. Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

2. Assessment Methods: Student Artifacts

Which student artifacts were used to determine if students achieved this outcome? Please identify the course(s) in which these artifacts were collected. Clarify if any such courses were offered a) online, b) at the Madrid campus, or c) at any other off-campus location.

1. Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.
    a. CYBR-5000 (Lab Projects 1, 2, 3)
    b. CYBR-5010 (Lab Projects 1, 2, 3)
2. Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.
    a. CYBR-5220 (Lab Project 1)

3. Assessment Methods: Evaluation Process

What process was used to evaluate the student artifacts, and by whom? Please identify the tools(s) (e.g., a rubric) used in the process and include them in/with this report.

Rubric (see attached)

4. Data/Results

What were the results of the assessment of the learning outcomes? Please be specific. Does achievement differ by teaching modality (e.g., online vs. face-to-face) or on-ground location (e.g., STL campus, Madrid campus, other off-campus site)?

Outcomes

- Results
  - Criteria 1
    - CYBR-5000 (Lab Project 1): A: 90%, B: 10%, C: 0%, D: 0%, F: 0%
    - CYBR-5000 (Lab Project 2): A: 90%, B: 5%, C: 5%, D: 0%, F: 0%
    - CYBR-5000 (Lab Project 3): A: 100%, B: 0%, C: 0%, D: 0%, F: 0%
    - CYBR-5010 (Lab Project 1): A: 90%, B: 10%, C: 0%, D: 0%, F: 0%
    - CYBR-5010 (Lab Project 2): A: 100%, B: 0%, C: 0%, D: 0%, F: 0%
    - CYBR-5010 (Lab Project 3): A: 90%, B: 10%, C: 0%, D: 0%, F: 0%
  - Criteria 2
    - CYBR-5220 (Lab Project 1): A: 90%, B: 5%, C: 5%, D: 0%, F: 0%
- This course was only delivered via online delivery.

5. Findings: Interpretations & Conclusions

What have you learned from these results? What does the data tell you?

Students enter the Cyber Security program with a variance in previous experience. CYBR-5000 and CYBR-5010 act as a course that baselines this experience and the lab projects provide hands on learning opportunities. The data is showing that despite previous experience with technical coursework, a student with less years of industry experience performs at or above the level of a student with this experience. This pattern continues into more administrative course work such as CYBR-5220 versus more technical courses such as CYBR-5000 and CYBR-5010/

6. Closing the Loop: Dissemination and Use of Current Assessment Findings

A. When and how did your program faculty share and discuss these results and findings from this cycle of assessment?

Retrospectives are held at the end of each sprint (8-week session) to review student grades and assignments that align to course objectives.

B. How specifically have you decided to use findings to improve teaching and learning in your program? For example, perhaps you've initiated one or more of the following:

Changes to the Curriculum or Pedagogies	• Course content • Teaching techniques • Improvements in technology • Prerequisites	• Course sequence • New courses • Deletion of courses • Changes in frequency or scheduling of course offerings
Changes to the Assessment Plan	• Student learning outcomes • Student artifacts collected • Evaluation process	• Evaluation tools (e.g., rubrics) • Data collection methods • Frequency of data collection

Please describe the actions you are taking as a result of the findings.

Course assignments are continually reviewed due to the technical nature of those assessments. Labs are also being designed to increase the hands on opportunities students have to illustrate course coverage. Rubrics measure both technical aptitude and the ability to convey those technical topics via technical writing.

If no changes are being made, please explain why.

N/A

7. Closing the Loop: Review of Previous Assessment Findings and Changes

A. What is at least one change your program has implemented in recent years as a result of assessment data?

Hands on labs were introduced.

B. How has this change/have these changes been assessed?

Hands on labs have been added to each course and assessment will continually be reviewed across both technical and non-technical course work in the MS in Cyber Security Program.

C. What were the findings of the assessment?

Student surveys have shown that students hands on labs are amongst the most rewarding and popular parts of the course that have helped enable them in their careers.

D. How do you plan to (continue to) use this information moving forward?

Labs that address timely technology topics will continually be integrated into course work.

IMPORTANT: Please submit any assessment tools and/or revised/updated assessment plans along with this report.