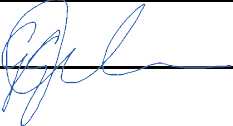


**Continuous Program Improvement (CPI)
Student Learning Outcomes (SLO)/Program Learning Outcomes (PLO)
Three Year Plan - 2023-2026**

Program name	Master of Science in Cybersecurity
Expected date of submission	June 30, 2024
Department chair/program director	Tokunbo Makanju
Dean's signature	Greg Gerber 

The Middle States Commission on Higher Education (MSCHE) Standard V, *Educational Effectiveness Assessment*, states: “Assessment of student learning and achievement demonstrates that the institution’s students have accomplished educational goals consistent with their program of study, degree level, the institution’s mission, and appropriate expectations for institutions of higher education.”

To ensure that New York Tech’s CPI process meets this standard, each department is requested to create a three-year assessment/evaluation plan to improve student learning for **each of their degree programs**. The plan should cover the following academic years: **2023-2024, 2024-2025, and 2025-2026**.

Each Program Learning Outcomes (PLO) CPI plan should include the following:

1. State/update each degree program’s **learning outcomes** based on the [Program Assessment Guidelines and Best Practices](#). The original Program Learning Outcome Assessment Plans and Reports are available here: http://www.nyit.edu/planning/academic_assessment_plans_reports.

The following list provides the program learning outcomes for Master of Science (MSc) in Cybersecurity Program:

1. **PLO 1:** Identify, formulate, and analyze the patterns and trends of threats as they apply to information systems, including methods, modes of preparation for attack, tactics, logistics, hazards, and vulnerabilities.
 2. **PLO 2:** Critically evaluate various technical/architectural solutions available to limit risk, mitigate the effects of hostile action and recover from attack.
 3. **PLO 3:** Design, implement and maintain software tools designed to support network security and systematically integrate these tools within multiple operating systems and platforms.
 4. **PLO 4:** Oversee the information assurance life cycle of an organization, including planning, acquisition, and implementation of secure infrastructures.
 5. **PLO 5:** Ensure compliance with security policy, legislation and market trends.
 6. **PLO 6:** Utilize mathematical and algorithmic solutions to complex information security problems.
 7. **PLO 7:** Apply probability and statistics for analysis.
2. Provide/update the **matrix of program learning outcomes** that indicates which learning outcomes are assessed in which courses. The original matrices are available here:
http://www.nyit.edu/planning/academic_assessment_plans_reports.

The following matrix provides the mapping of program learning outcomes for each course in Cybersecurity program:

Course	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6	PLO 7
CSCI 620		x	x				
CSCI 651						x	x
CSCI 657						x	x
CSCI 662		x			x		
CSCI 690			x	x		x	
INCS 615	x	x		x			
INCS 618	x			x	x		
INCS 712		x					
INCS 735		x	x		x		
INCS 741		x					
INCS 745	x	x					
INCS 775	x	x			x		
INCS 810	x	x	x				
INCS 870		x	x	x	x		x
INCS 880		x	x	x	x		x

- Describe the **method of assessment and measurement instruments** (e.g., rubric, exam items, scoring guide for a particular task, supervisor evaluation form, and standardized assessment tool). Note: Direct evidence of student learning is required; both direct and indirect evidence are strongly recommended. ***[Direct evidence of student learning includes but is not limited to: course assignments, portfolios, internship evaluations, capstone course work, thesis papers, research projects, standardized tests, etc. Indirect evidence of student learning includes but is not limited to: student surveys, interviews, alumni surveys, employer surveys, focus***

groups, students' reflections, etc.]

The following are the metrics that will be used for evaluating the program learning outcomes above. It specifies the definition, what, how and when for measuring the learning outcome for each course.

- **Definition:** how well the courses meet the learning outcomes as defined in the matrix.
- **What:** There will be both direct and indirect assessment of the learning outcomes
 - **Indirect Assessment:** Responses to the following statements from the student course evaluation survey:
 - The course objectives as stated in the syllabus were met. (Question 10)
 - Instructor clearly stated the objectives of the course and each topic. (Question 7)
 - The content of the course and the material covered was directly related to the objectives of the course. (Question 8)
 - **Direct Assessment:** Reported performance statistics provided by faculty on specific assessments related to each PLO.
- **How:**
- **Indirect Assessment:** The average of each course's responses to the above questions for all instructors who teach the course. This will provide a score between 0 -5 that will be judged based on the rubric below:

	Rubric	Score
E-Excellent	Students assess that the course fully demonstrates/accomplishes the learning outcome objectives	$S \geq 4$
G-Good	Students assess that the course mostly demonstrates/accomplishes the learning outcome objectives	$3 \leq S < 4$
U-Unsatisfactory	Students assess the course does not or minimally demonstrates/accomplishes the learning outcome objectives	$S < 3$

- **Direct Assessment:** Each faculty member will provide an EGMU (Excellent, Good, Minimal and Unsatisfactory) score for the performance of students in their class on the identified assessments related to the learning outcomes. The EGMU Vector is obtained as follows:
 - **3 (Excellent):** Demonstrates a complete and accurate understanding of the important concepts
 - **2 (Good):** Applies appropriate strategy or concepts with no significant errors
 - **1 (Minimal):** Displays an incomplete understanding of the important concepts and has some notable

misconceptions; makes a number of errors when performing important strategies or skills but can complete a rough approximation of them

- **0 (Unsatisfactory):** Demonstrates severe misconceptions about the important concepts; makes many critical errors.

For example, a typical EGMU vector for a class with 19 students on the identified assessment related to the PLO might be (8, 9, 1, 1) which would signify that 8 students demonstrated a complete and accurate understanding, while 9 students applied appropriate strategies etc. The average score in this case being $43/19 = 2.26$ which is Good.

Vancouver Cybersecurity faculty have decided that our department will be requiring, as a minimum, an EGMU score of 2.0 for each (PO). This value was chosen because it represents a grade of B- or B

- **Supporting documents:** the instructor of each course needs to provide the documents that support how they meet the specific program learning objectives assigned to the course. They need to provide methods of assessment, and measurement instruments (e.g., rubric, exam items, scoring guide for a particular task, supervisor evaluation form, and standardized assessment tool).
- **When:**
 - End of each academic year – each year ends in August:
 - Faculty with courses that are linked in the matrix to the learning objectives to be evaluated for the year need will need to update the shared spreadsheet with the questions' scores (from course evaluations), EGMU scores for each PLO and supporting documents.
 - A meeting of faculty will be called to discuss the results and a report will be prepared.
 - Note: the report will be shared in a shared folder.

4. A **timeline** of when each PLO will be assessed, for example:

The following timeline provides the plan for evaluation of program learning objectives in a three academic year period.

MS Cybersecurity			
Program Learning/Student Outcomes	AY 23-24	AY 24-25	AY 25-26
1. Identify, formulate, and analyze the patterns and trends of threats as they apply to information systems, including methods, modes of preparation for attack, tactics, logistics, hazards, and vulnerabilities	•		
2. Critically evaluate various technical/architectural solutions available to limit risk, mitigate the effects of hostile action and recover from attack	•		
3. Design, implement and maintain software tools designed to support network security and systematically integrate these tools within multiple operating systems and platforms		•	
4. Oversee the information assurance life cycle of an organization, including planning, acquisition, and implementation of secure infrastructures		•	
5. Ensure compliance with security policy, legislation and market trends		•	
6. Utilize mathematical and algorithmic solutions to complex information security problems			•
7. Apply probability and statistics for analysis.			•

5. **Faculty working as a team** is essential in program learning outcome assessment. Please provide a **brief description** of how faculty are involved in the creation of this assessment plan and how the results will be communicated to all stakeholders.

The plan was prepared over a period lasting over six months during the 2022/23 and 2023/24 AY years. The plan was discussed during faculty meetings and the plan document was provided in a shared drive where faculty had access to edit and make comments on the plan. The final report will be sent to all faculty members via email.