Neumann University Program Assessment Plan

Program Name: Cybersecurity		**Program Liaison: Tom Dodds**
Division: Business and Information Management		**3-Year Cycle Span: AY 23/24 to AY 25/26**

Student Learning Outcome Upon successful completion of the Cybersecurity Program, the student will:	**LO 1** Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats. **Bloom: Comprehension**	**LO 2** Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth. **Bloom: Application**	**LO 3** Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems. **Bloom: Application**	**LO 4** Evaluate information security trends and practices and how to measure the performance of security systems within an organization. **Bloom: Analysis**	**LO 5** Discover how to maintain confidentiality, integrity, and availability of secure systems. **Bloom: Analysis**	**LO 6** Understand how to decipher and code security tools using Python. **Bloom: Application**	**LO 7** Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks. **Bloom: Application**	**LO 8** Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers. **Bloom: Application**
Core Learning Outcome(s):	Comprehension	Comprehension	Comprehension	Comprehension	Comprehension	Comprehension	Comprehension	Comprehension
Course Mapping and Related IDEA Objective(s):	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material (to improve thinking, problem solving, and decisions)	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material (to improve thinking, problem solving, and decisions) Developing specific skills, competencies, and	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material (to improve thinking, problem solving, and decisions)	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material (to improve thinking, problem solving, and decisions) Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course.	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material (to improve thinking, problem solving, and decisions)	Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories) Learning to apply course material (to improve thinking, problem solving, and decisions) Developing specific skills, competencies, and	Gaining a basic understandin of the subjec (e.g., factual knowledge, methods, principles, generalizatio s, theories) Learning to apply course material (to improve thinking, problem

Neumann University Program Assessment Plan

Student Learning Outcome Upon successful completion of the Cybersecurity Program, the student will:	**LO 1** Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats. **Bloom: Comprehension**	**LO 2** Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth. **Bloom: Application**	**LO 3** Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems. **Bloom: Application**	**LO 4** Evaluate information security trends and practices and how to measure the performance of security systems within an organization. **Bloom: Analysis**	**LO 5** Discover how to maintain confidentiality, integrity, and availability of secure systems. **Bloom: Analysis**	**LO 6** Understand how to decipher and code security tools using Python. **Bloom: Application**	**LO 7** Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks. **Bloom: Application**	**LO 8** Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers. **Bloom: Application**
	Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course. Learning how to find, evaluate and use resources to explore a topic in depth.	points of view needed by professionals in the field most closely related to this course. Acquiring skills in working with others as a member of a team.	Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course. Learning to analyze and critically evaluate ideas, arguments, and points of view	Learning to analyze and critically evaluate ideas, arguments, and points of view	(to improve thinking, problem solving, and decisions) Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course.	Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course. Developing creative capacities (designing, inventing and coding creative solutions)	points of view needed by professionals in the field most closely related to this course. Learning appropriate methods for collecting, analyzing, and interpreting information.	solving, and decisions) Developing specific skill competencie and points of view needed by professional in the field most closely related to thi course. Learning to apply knowledge and skills to benefit other or serve the public good.

Neumann University Program Assessment Plan

Student Learning Outcome Upon successful completion of the Cybersecurity Program, the student will:	**LO 1** Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats. **Bloom: Comprehension**	**LO 2** Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth. **Bloom: Application**	**LO 3** Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems. **Bloom: Application**	**LO 4** Evaluate information security trends and practices and how to measure the performance of security systems within an organization. **Bloom: Analysis**	**LO 5** Discover how to maintain confidentiality, integrity, and availability of secure systems. **Bloom: Analysis**	**LO 6** Understand how to decipher and code security tools using Python. **Bloom: Application**	**LO 7** Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks. **Bloom: Application**	**LO 8** Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers. **Bloom: Application**
					Learning how to find, evaluate and use resources to explore a topic in depth.			
Academic Year for Assessment: each LO will be assessed.	**AY 23/24**	**AY 23/24**	**AY 24/25**		**AY 24/25**			
Formative Assessment	CBR 201 70% of students will score 80% or higher on the comprehensive final exam.	CBR 202 70% of students will score 80% or higher on the final exam.	CBR 203 70% of students will solve the final capture the flag exercise.		CBR 301 70% of the students will successfully complete and prese results as part of a real-world cybersecurity incident response.			

Neumann University Program Assessment Plan

Student Learning Outcome Upon successful completion of the Cybersecurity Program, the student will:	**LO 1** Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats. **Bloom: Comprehension**	**LO 2** Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth. **Bloom: Application**	**LO 3** Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems. **Bloom: Application**	**LO 4** Evaluate information security trends and practices and how to measure the performance of security systems within an organization. **Bloom: Analysis**	**LO 5** Discover how to maintain confidentiality, integrity, and availability of secure systems. **Bloom: Analysis**	**LO 6** Understand how to decipher and code security tools using Python. **Bloom: Application**	**LO 7** Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks. **Bloom: Application**	**LO 8** Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers. **Bloom: Application**
Summative Assessment	**CBR 202** 70% of students will score 80% or higher on the semester-long internal, external and network security design projects.	**CBR 202** 70% of students will score 80% or higher on the semester-long internal, external and network security design projects.	**CBR 301** 70% of students will score 80% or higher on Incident response plan.		**CBR 301 Selection of Cyber Incident Response Exercises:** 70% of students will score 80% or higher on the result documented response to a cyber incident.			

Neumann University Program Assessment Plan

Student Learning Outcome Upon successful completion of the Cybersecurity Program, the student will:	**LO 1** Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats. **Bloom: Comprehension**	**LO 2** Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth. **Bloom: Application**	**LO 3** Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems. **Bloom: Application**	**LO 4** Evaluate information security trends and practices and how to measure the performance of security systems within an organization. **Bloom: Analysis**	**LO 5** Discover how to maintain confidentiality, integrity, and availability of secure systems. **Bloom: Analysis**	**LO 6** Understand how to decipher and code security tools using Python. **Bloom: Application**	**LO 7** Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks. **Bloom: Application**	**LO 8** Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers. **Bloom: Application**

Neumann University Program Assessment Plan

<table>
<tr>
<td><b>Student Learning Outcome</b> Upon successful completion of the Cybersecurity Program, the student will:</td>
<td><b>LO 1</b>
Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats.
<b>Bloom: Comprehension</b></td>
<td><b>LO 2</b>
Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth.
<b>Bloom: Application</b></td>
<td><b>LO 3</b>
Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems.
<b>Bloom: Application</b></td>
<td><b>LO 4</b>
Evaluate information security trends and practices and how to measure the performance of security systems within an organization.
<b>Bloom: Analysis</b></td>
<td><b>LO 5</b>
Discover how to maintain confidentiality, integrity, and availability of secure systems.
<b>Bloom: Analysis</b></td>
<td><b>LO 6</b>
Understand how to decipher and code security tools using Python.
<b>Bloom: Application</b></td>
<td><b>LO 7</b>
Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks.
<b>Bloom: Application</b></td>
<td><b>LO 8</b>
Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers.
<b>Bloom: Application</b></td>
</tr>
<tr>
<td><b>Indirect Evidence:</b>
IDEA Example:
Student ratings on relevant objectives will be at or above the IDEA norm.</td>
<td>In courses where objectives are noted as Essential or Important, at least 70% of students will rate themselves as making Moderate Progress or better.
<table>
<tr><td>Idea Objective</td><td>Cou</td></tr>
<tr><td>1</td><td>CB
CB</td></tr>
<tr><td>3</td><td>CB
CB</td></tr>
<tr><td>4</td><td>CB
CB</td></tr>
<tr><td>5</td><td>CB</td></tr>
<tr><td>9</td><td>CB</td></tr>
</table>
</td>
<td>In courses where objectives are noted as Essential or Important, at least 70% of students will rate themselves as making Moderate Progress or better.
<table>
<tr><td>Idea Objective</td><td>Cours</td></tr>
<tr><td>1</td><td>CBR2
CBR2</td></tr>
<tr><td>3</td><td>CBR2
CBR2</td></tr>
<tr><td>4</td><td>CBR2
CBR2</td></tr>
<tr><td>5</td><td>CBR</td></tr>
<tr><td>9</td><td>CBR</td></tr>
</table>
</td>
<td colspan="2">In courses where objectives are noted as Essential or Important, at least 70% of students will rate themselves as making Moderate Progress or better.
<table>
<tr><td>Idea Objective</td><td>Course</td></tr>
<tr><td>1</td><td>CBR301/
CBR302</td></tr>
<tr><td>3</td><td>CBR301/
CBR302</td></tr>
<tr><td>4</td><td>CBR301/
CBR302</td></tr>
<tr><td>6</td><td>CBR 302</td></tr>
<tr><td>11</td><td>CBR 301</td></tr>
</table>
</td>
<td colspan="4">In courses where objectives are noted as Essential or Important, at l students will rate themselves as making Moderate Progress or bette
<table>
<tr><td>Idea Objective</td><td>Course</td></tr>
<tr><td>1</td><td>CBR301/
CBR302</td></tr>
<tr><td>3</td><td>CBR301/
CBR302</td></tr>
<tr><td>4</td><td>CBR301/
CBR302</td></tr>
<tr><td>6</td><td>CBR 302</td></tr>
<tr><td>11</td><td>CBR 301</td></tr>
</table>
</td>
</tr>
</table>

Neumann University Program Assessment Plan

Student Learning Outcome Upon successful completion of the Cybersecurity Program, the student will:	**LO 1**	**LO 2**	**LO 3**	**LO 4**	**LO 5**	**LO 6**	**LO 7**	**LO 8**
	Understand and articulate basic security concepts and models and how to defend against persistent and constantly evolving threats. **Bloom: Comprehension**	Apply current technology, tools, and systems as part of the process of implementing a security model based on defense in depth. **Bloom: Application**	Analyze cybersecurity risks at all levels while obtaining skills essential to designing inherently secure systems. **Bloom: Application**	Evaluate information security trends and practices and how to measure the performance of security systems within an organization. **Bloom: Analysis**	Discover how to maintain confidentiality, integrity, and availability of secure systems. **Bloom: Analysis**	Understand how to decipher and code security tools using Python. **Bloom: Application**	Implement and understand both continuous and real-time network monitoring at all levels to analyze and detect malware and other cyberattacks. **Bloom: Application**	Learn to assess computer system security by using ethical hacking techniques: social engineering, vulnerability scans, reconnaissan e, etc. to repe hackers. **Bloom: Application**

Neumann University Program Assessment Plan

Neumann University Program Assessment Plan

NOTE: This page is a tool to be used by the Program Liaison to ensure that all courses are included in the assessment plan.
It is not a required item.

__________________ Program Course List and Corresponding Assessments

COURSES	CBR 201 - Introduction to Cybersecurity	CBR 202 - Cybersecurity Essentials	CBR 203 - Application Security, and Cryptography	CBR 301 – Incident Response (Assessments, Audits and Risk Management)	CBR 302 Introduction to Python Programming	CBR 401 - Ethical Hacking and Penetration Testing	CBR 402 - Intrusion Detection and Forensics
Formative	LO1 Final exam	LO2 Final exam LO5 Final exam LO6 Final exam	LO3 capture the flag	LO4 real world incident response exercise		LO7 Final lab	LO8 Capstone labs
Summative		LO1 Semester Project LO2 Semester Project LO5 Semester Project		LO3 Incident response plan LO4 evaluate modern trends	LO6 Final program	LO7 Final lab	LO8 Capture the flag
Indirect							