

EXHIBIT B



BOARD OF TRUSTEES

Bylaw, Policy, and Curriculum Committee Agenda Items

To: Board of Trustees
From: Office of the President
Date: February 18, 2021

The following Bylaw, Policy, and Curriculum Committee items are recommended to the Ocean County College Board of Trustees for approval at its meeting on **Thursday, February 25, 2021**:

1. Recommend amendments to the following Board Bylaws:
 - a. Bylaw #1120, Mission of the College (**Exhibit B-1**)
 - b. Bylaw #1252.2, Bylaw, Policy, and Curriculum Committee (**Exhibit B-2**)

As required by Policy #1370, Amendments to Bylaws, the proposed Bylaw amendments were introduced at the January 28, 2021, Board meeting and distributed to the Trustees ten days in advance of this meeting.

2. Recommend approval of the following items as accepted by the College Senate at its meeting on February 4, 2021:
 - a. New Certificate
 - 1) Certificate of Completion in Cybersecurity (**Exhibit B-3**)
 - b. New Courses
 - 1) CSIT 240, Ethical Hacking: Hacker Techniques and Tools (**Exhibit B-4**)
 - 2) CSIT 241, Cybersecurity Legal and Regulatory (**Exhibit B-5**)

EXHIBIT B-1

Ocean County College, Toms River, NJ

BYLAWS FOR THE OPERATION OF
THE BOARD OF TRUSTEES
GENERAL
Mission of the College #1120

BYLAW

Ocean County College, an innovative academic leader, provides affordable, student-centered, high-quality educational experiences that empower diverse learners to succeed.

To achieve its mission, OCC invests in and fosters academic, economic, and cultural excellence and ensures financial strength by generating multiple revenue streams, engaging in national and international university and corporate partnerships, and cultivating a technologically progressive and entrepreneurial spirit.

~~It is the mission of Ocean County College to foster excellence and a caring environment through its commitment to:~~

- ~~o Offer comprehensive educational programs that develop intentional learners of all ages and ensure the full assessment of student learning in these programs;~~
- ~~o Provide broadly based student support, starting from our initial contact with every individual, regardless of his or her unique needs;~~
- ~~o Measure employee attitudes toward the workplace and student attitudes toward the learning experience and make responsive adjustments in institutional strategies;~~
- ~~o Provide a well designed campus and facilities with advanced technology;~~
- ~~o Address our human resource needs by recruiting and hiring highly qualified people and continuing to develop the potential of each employee;~~
- ~~o Generate and manage fiscal resources to best serve strategic priorities;~~
- ~~o Organize a leadership team committed to outreach, development, engagement, institutional effectiveness, and a fully realized implementation of the college's vision;~~
- ~~o Reach out to members of the Ocean County community and beyond in order to create meaningful, fulfilling, and mutually beneficial partnerships.~~

ADOPTED: February 22, 1965

Revised: November 7, 1983

Revised: August 21, 1995

Revised: December 13, 1999

Revised: December 13, 2004

Revised: February 25, 2021

EXHIBIT B-2

Ocean County College, Toms River, NJ

BYLAWS FOR THE OPERATION
OF THE BOARD OF TRUSTEES
ORGANIZATION
Committees of the Board
Standing Committees
Bylaws, Policy, and Curriculum #1252.2

BYLAW

The Bylaws, Policy, and Curriculum Committee shall be responsible for and shall make recommendations to the full Board regarding the following areas:

The policy development for the total organization and operation of Ocean County College.

The development and approval of the program offerings.

The determination of the need for new programs.

The evaluation of the effectiveness of the programs being offered.

The oversight of the Board's self-assessment procedures, as recommended by the Office of Institutional Planning, Effectiveness, and Compliance to ensure compliance with the Middle States Commission on Higher Education.

ADOPTED: February 22, 1965
Revised: November 7, 1983
Revised: April 28, 2008
Revised: February 25, 2021

REVIEWED: March 5, 1991

EXHIBIT B-3



**BOARD OF TRUSTEES
RESOLUTION**

WHEREAS, Ocean County College desires to offer a new Certificate of Completion in Cybersecurity (CIP Code 522101); and

WHEREAS, the Certificate of Completion in Cybersecurity is designed to provide students with the fundamentals necessary to pursue a career as an information security analyst; and

WHEREAS, this certificate program will provide students with the necessary background to prepare for and acquire recognized industry certifications; and

WHEREAS, the U.S. Bureau of Labor Statistics estimated 131,000 positions in information security in 2019, with one-third of the positions being unfilled, and projected a 31% increase in the number of positions in the next ten years; and

WHEREAS, the credits from this certificate program may be applied toward an associate degree; and

WHEREAS, this certificate program consists of 19 credits;

NOW, THEREFORE, BE IT RESOLVED that the Ocean County College Board of Trustees, at its meeting on February 25, 2021, approves the Certificate of Completion in Cybersecurity.

February 25, 2021

Stephan R. Leone
Secretary

Program Type

Certificate of Completion

Program Title

Certificate of Completion in Cybersecurity

Academic School

Science, Technology, Engineering, Mathematics

Effective Catalog Year

2021-2022

Program Code

CC.CYBER

CIP Code

522101 - Telecommunications Management.

Program Description

The program description should be developed with the program goals in mind. Also, consider that it will be what goes into the college catalog and will represent the program publicly in the future. Try to make it readable for students and informative but not too busy. This should give a brief synopsis of what the program offers in terms of content, transfer, and career.

The Ocean County College Certificate of Completion in Cybersecurity provides students with the fundamentals necessary to pursue a career as an information security analyst. It is the common foundation for alternative Associate's Degree paths, both direct to industry, and with articulation into a four-year university programs. It provides the background necessary for students to prepare for and acquire recognized industry certifications as well.

The US Bureau of Labor Statistics estimated 131,000 positions in information security in 2019, growing by 31% in the next ten years. Furthermore, the chair of the House Subcommittee on Research and Technology estimates that 1/3 of such positions are going unfilled and require multiple pathways, including certifications and internship programs to fill the void.

Program Learning Outcomes

Students who successfully complete this program will be able to:	
PLO1	Demonstrate a knowledge of the fundamental concepts of computer, network, application and information security. Student will possess knowledge on a broad category of security topics such as security controls, basic cryptography concepts, secure network architectures, protocols and cyber-attacks.

Students who successfully complete this program will be able to:	
PLO2	Demonstrate the ability to assess and maintain the security of applications, operating systems, networks and business data. This skill will be used to identify security weaknesses and mitigate risk. This includes knowledge of how to develop and deploy secure applications. Students will also be able to demonstrate and apply certified ethical hacking principles as it relates to this outcome.
PLO3	Demonstrate a knowledge of the various Cloud Computing services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The student will be trained in the advantages and disadvantages of migrating to a Cloud based environment as well as maintaining Cloud based services so that they are secure. Students will also understand how to evaluate perimeter security from a cloud and network perspective.
PLO4	Explain the concepts of Organization security in the following areas: policy, data security, data privacy and personnel management. This includes knowledge in the areas of risk management, resiliency, automation and disaster recovery strategies as well as legal and regulatory expertise.

Learning Outcomes Display (show only)

Course Code	PLO 1	PLO 2	PLO 3	PLO 4
FirstSemester				
CSIT 144				
CSIT 185				
CSIT 200				
SecondSemester				
CSIT 277				
CSIT 240				
CSIT 241				

Required Qualifications

Plan of Study Grid

First Semester	Credit Hours
<u>CSIT 144</u> Introduction to Operating System Using Unix	3
<u>CSIT 185</u> Networking I	3
<u>CSIT 200</u> Information Security Fundamentals	3
Credit Hours	9
Second Semester	
<u>CSIT 277</u> Introduction to Cloud Computing	4
<u>CSIT 240</u> Ethical Hacking: Hacker Techniques and Tools	3
<u>CSIT 241</u> Cybersecurity Legal and Regulatory Overview	3
Credit Hours	10
Total Credit Hours	19

Degree Requirements Breakdown

GCOM

Course Code & Title	Credits
N/A	0

GHUM

Course Code & Title	Credits
N/A	0

GSOC

Course Code & Title	Credits
N/A	0

GSOC/ GHUM

Course Code & Title	Credits
N/A	0

GMAT/ GSCI/ GTEC

Course Code & Title	Credits
N/A	0

General Education

Course Code & Title	Credits
N/A	0

Concentration Courses

Course Code & Title	Credits
CSIT 144 - Introduction to Operating System using Unix	3
CSIT 185 - Networking I	3
CSIT 200 - Information Security Fundamentals	3
CSIT 277 - Cloud Computing	4
CSIT 240 - Ethical Hacking: Hacker Techniques and Tools	3
CSIT 241 - Cybersecurity Legal and Regulatory Overview	3

Elective Courses

Course Code & Title	Credits
N/A	0

Reviewer Comments

EXHIBIT B-3

Cynthia Fallon (cfallon) (Tue, 24 Nov 2020 16:38:58 GMT): Rollback: Sending this back at your request.

Susan O'Connor (soconnor) (Fri, 22 Jan 2021 14:21:38 GMT): Rollback: need to add in course numbers

Key: 74

EXHIBIT B-4

CSIT 240 : Ethical Hacking: Hacker Techniques and Tools

1. Course Information

Subject

CSIT - Computer Science/ Information Technology

School

Science, Technology, Engineering, Mathematics

Course Title

Ethical Hacking: Hacker Techniques and Tools

2. Hours

Semester Hours

3

Lecture

3

Lab

0

Practicum

0

3. Catalog Description

For display in the online catalog

This course explores the fundamental concepts of hacker techniques and tools which are used in the field of Ethical Hacking. Topics to be covered include the planning, sanctioning, assurance and execution of an ethical hack, including an understanding of the critical categories of attack techniques that would be used. The course will also review the various software, application, network, and platform vulnerabilities that would be the focus of the attacks. Lab activities will provide students with practical experiences in ethical hacking. Open lab time is required.

4. Requisites

Prerequisites

CSIT 200 with a grade of C or higher.

Corequisites

5. Course Type

Course Type for Perkins Reporting

vocational (approved for Perkins funding)

6. Justification

Describe the need for this course

This course will be a requirement toward a Cybersecurity Certificate of Completion as part of a curriculum designed to address the “Cyber Threats (CT)” Knowledge Unit requirement for OCC qualification as a National Center of Academic Excellence in Cyber Defense (CAE-CD). It will also prepare the student to test to for certification by the EC-Council as a Certified Ethical Hacker (CEH). The CEH certification is recognized for the DoD's computer network defense Service Providers (CND-SP's), a specialized personnel classification within the United States Department of Defense's information assurance workforce.

7. General Education

Will the college submit this course to the statewide General Education Coordinating Committee for approval as a course, which satisfies a general education requirement?

No

If the course does not satisfy a general education requirement, which of the following does it satisfy:

Program-specific requirement

This course is recommended for

8. Consistency with the Vision and Mission Statements, the Academic Master Plan, and the strategic initiatives of the College

Please describe how this course is consistent with Ocean County College's current Vision Statement, Mission Statement, Academic Master Plan, and the strategic initiatives of the College:

Add item	
1	Demonstrating the college’s commitment to offer comprehensive educational programs that develop intentional learners of all ages. (Mission Statement)
2	Seeking to ensure that students will thrive in an increasingly diverse and complex world. (Vision Statement)
3	Preparing students for successful transfer to other educational institutions and/or for entrance into the workforce. (Academic Master Plan)
4	Seeking to empower students through the mastery of intellectual and Practical Skills. (Academic Master Plan)
5	Challenging students to transfer information into knowledge and knowledge into action. (Academic Master Plan)

9. Related Courses at Other Institutions

Comparable Courses at NJ Community Colleges

Institution

Brookdale CC

Course Title

Hacker Techniques, Tools, and Incident Handling

Course Number

NETW238

Number of Credits

3

Comments

Institution

Rowan College at Burlington County

Course Title

Ethical Hacking Fundamentals

Course Number

CIS-218

Number of Credits

3

Comments

Institution

County College of Morris

Course Title

Ethical Hacking and Systems Defense

Course Number

CMP-243

Number of Credits

3

Comments

Institution

Essex County College

Course Title

Network Defense and Countermeasures

Course Number

CSC 226

Number of Credits

4

Comments

Institution

Hudson County CC

Course Title

Ethical Hacking

Course Number

CSC 245

Number of Credits

3

Comments

Institution

Mercer County CC

Course Title

Ethical Hacking

Course Number

NET 245

Number of Credits

3

Comments

Institution

Raritan Valley CC

Course Title

Ethical Hacking and Penetration Testing

Course Number

NTWK 290

Number of Credits

3

Comments

Transferability of Course

Georgian Court University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
EC 56 Elective - 3 Credits	Elective	

Kean University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CPSX1003 - Computer Science Free Elective or TECHX2002 - Technology Elective - 3 Credits	Elective	

Monmouth University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CS002 - 200 Level Computer Science Elective - 3 Credits	Elective	

Rowan University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
Elective, EC, 3 cr.	Elective	

Rutgers - New Brunswick, Mason Gross School of the Arts

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
		Will not transfer

Stockton University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CSISEC - Computer Science and Information Systems Elective - Elective 3 Credits		

If not transferable to any institution, explain:

Rutgers: Students who take this course as a part of an AA or AS degree can receive Elective credit

10. Course Learning Outcomes

Learning Outcomes

Students who successfully complete this course will be able to:	
CLO1	Develop a plan for an ethical hack for proposal and review by parties responsible for protecting corporate systems.
CLO2	Specify the skills, tools and techniques required for ethical hacking.
CLO3	List various avenues of attacks including the categories of compromise, the critical assets, the elements of a system, cloud platforms and the system lifecycle which covers when attacks can occur.
CLO4	Classify details of the various attack vulnerabilities including software, authentication, network, denial of service, platform, and social engineering vulnerabilities.
CLO5	Demonstrate ways to avoid detection during an ethical hacking exercise.
CLO6	Leverage resources from the various Hacker networks, forums and information resources.

11. Topical Outline

(include as many themes/skills as needed)

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
TO1	Being an Ethical Hacker 1) The Demand for	Hands-on, Lab exercises	Exam	CL01

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
	Ethical Hacking 2) The Dangers and Penalties for Unethical Hacking 3) Contracting and Planning the Ethical Hack 4) Creating a Monster – Case Study: The Morris Worm			
TO2	Avenues of Attack 1) Categories of Compromise 2) Critical Assets 3) The Elements of a System 4) Cloud (ETSI NFV) Architecture Elements	Hands-on, Lab exercises	Exam	CL01, CL02
TO3	Attack Categories 1) Software Vulnerabilities 2) Authentication Vulnerabilities 3) Network Vulnerabilities 4) Denial of Service Vulnerabilities 5) Client Platform Vulnerabilities 6) Covert Channels 7) Social Engineering	Hands-on, Lab exercises	Lab assignment	CL01, CL03
TO4	Avoiding Detection 1) Logs and Audit Trails, 2) Intrusion Detection Systems, 3) Caller ID, 4) Establishing E-mail Accounts, 5) Bots and Zombies,	Hands-on, Lab exercises	Exam	CL01, CL04

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
TO5	6) Honeypots, 7) Security Operations Centers. Hacker Networks and Information Sources 1) Computer Emergency Response Team (CERT) 2) Certified Ethical Hacker (CEH) Certification (http://eccouncil.org) 3) Google’s Bug Hunter University 4) Hacktivity	Hands-on, Lab exercises	Exam	CL01, CL05

12. Methods of Instruction

In the structuring of this course, what major methods of instruction will be utilized?

- o Class lecture
- o Discussion
- o Demonstrations
- o Lab assignments
- o Programs and online presentations

13. General Education Goals Addressed by this Course (this section is to fulfill state requirements)

Information

Communication-Written and Oral

Quantitative Knowledge and Skills

Scientific Knowledge and Reasoning

Technological Competency

Yes

Related Course Learning Outcome

CL01-CL01

Related Outline Component

TO1-TO5

Assessment of General Education Goal (Recommended but not limited to)

Exam, Project

Information Literacy

Society and Human Behavior

Humanistic Perspective

Historical Perspective

Global and Cultural Awareness

Ethical Reasoning and Action

Independent/Critical Thinking

Yes

Related Course Learning Outcome

CL01, CL03

Related Outline Component

TO1-TO5

Assessment of General Education Goal (Recommended but not limited to)

Exam, Project

14. Needs

Instructional Materials (text etc.):

Appropriate textbooks and/or Open Educational Resources will be selected. Class notes, presentations, software and online materials.

Technology Needs:

College Portal and/or College Distance Learning Platform and/or Textbook or Instructor Website.

Human Resource Needs (Presently Employed vs. New Faculty):

Presently Employed Faculty.

Facility Needs:

Laboratory classrooms equipped with computer workstations. Isolated network and computers to demonstrate cybersecurity principles, security and attacks. Podium computer similarly equipped plus the ability to present audio-video presentations to the class.

Library needs:

None

15. Grade Determinants

The final grade in the course will be the cumulative grade based on the following letter grades or their numerical equivalents for the course assignments and examinations

A: Excellent

B+: Very Good

B: Good

C+: Above Average

C: Average

D: Below Average

F: Failure

I: Incomplete

R: Audit

For more detailed information on the Ocean County College grading system, please see Policy #5154.

Reviewer Comments

Key: 2177

EXHIBIT B-5

CSIT 241 : Cybersecurity Legal and Regulatory Overview

1. Course Information

Subject

CSIT - Computer Science/ Information Technology

School

Science, Technology, Engineering, Mathematics

Course Title

Cybersecurity Legal and Regulatory Overview

2. Hours

Semester Hours

3

Lecture

3

Lab

0

Practicum

0

3. Catalog Description

For display in the online catalog

This course reviews the various government and industry-specific laws, regulations and standards that govern the policies of an enterprise Cybersecurity program. This course prepares students to be both authors and participants in the definition, implementation, execution and assurance of such policies across a range of career areas and roles, included but not limited to Security Specialist, Government Administrator, Human Resources Professional, and Law Enforcement Officer.

4. Requisites

Prerequisites

CSIT 200 with a grade of C or higher.

Corequisites

5. Course Type

Course Type for Perkins Reporting

vocational (approved for Perkins funding)

6. Justification

Describe the need for this course

This course will be a requirement toward a Cybersecurity Certificate of Completion as part of a curriculum designed to address the “Policy, Legal and Ethics (PLE)” Knowledge Unit requirement for OCC qualification as a National Center of Academic Excellence in Cyber Defense (CAE-CD).

7. General Education

Will the college submit this course to the statewide General Education Coordinating Committee for approval as a course, which satisfies a general education requirement?

No

If the course does not satisfy a general education requirement, which of the following does it satisfy:

Program-specific requirement

This course is recommended for

8. Consistency with the Vision and Mission Statements, the Academic Master Plan, and the strategic initiatives of the College

Please describe how this course is consistent with Ocean County College's current Vision Statement, Mission Statement, Academic Master Plan, and the strategic initiatives of the College:

Add item	
1	Demonstrating the college’s commitment to offer comprehensive educational programs that develop intentional learners of all ages. (Mission Statement)
2	Seeking to ensure that students will thrive in an increasingly diverse and complex world. (Vision Statement)

Add item	
3	Preparing students for successful transfer to other educational institutions and/or for entrance into the workforce. (Academic Master Plan)
4	Seeking to empower students through the mastery of intellectual and Practical Skills. (Academic Master Plan)
5	Challenging students to transfer information into knowledge and knowledge into action. (Academic Master Plan)

9. Related Courses at Other Institutions

Comparable Courses at NJ Community Colleges

Institution

Sussex County CC

Course Title

Cyber Law

Course Number

CYBR102

Number of Credits

3

Comments

Institution

Union County College

Course Title

Cyber Law and Ethics

Course Number

CST215

Number of Credits

3

Comments

Transferability of Course

Georgian Court University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
EC "56" – Elective Credit – 3 Credits	Elective	

Kean University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CJ3710 Cyber Policy – 3 Credits	Elective	

Monmouth University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CS002 – 200-Level Computer Science Elective – 3 Credits	Elective	

Rowan University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CS01077 Computer Science GE Elective – 3 Credits	Elective	

Rutgers - New Brunswick, Mason Gross School of the Arts

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
		Will not transfer

Stockton University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CRIMEC – Criminal Justice Elective – 3 Credits CSISEC – Computer Science and Info System Elective – 3 Credits	Elective	

If not transferable to any institution, explain:

Rutgers: Students who take this course as a part of an AA or AS degree can receive Elective credit

10. Course Learning Outcomes

Learning Outcomes

Students who successfully complete this course will be able to:	
CLO1	Identify the Cybersecurity laws, standards and regulations that apply to a specific enterprises and industries,
CLO2	Apply the requirements, processes and approaches necessary to address the various legal and regulatory requirements in an enterprise Cybersecurity Policy,
CLO3	Explain the statutes and penalties that apply to Cybersecurity crimes as specified in the various laws,
CLO4	Apply the various standards, models and processes to identify and analyze Cybersecurity risks and specify mitigation plans and countermeasures,
CLO5	Describe the role of Cybersecurity policy in various industry areas and careers.

11. Topical Outline

(include as many themes/skills as needed)

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
TO1	Introduction to Security Policy 1) Defining Security Policy 2) Establishing a	Hands-on	Exam	CL01, CL02

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
	Security Policy 3) Identifying Relevant Laws and Regulations 4) The Security Policy Lifecycle 5) The Costs of Non- Compliance Overview of Key Federal Cybersecurity Laws and Initiatives 1) Cybersecurity Fraud and Abuse Act (CSFAA) (1986) 2) Presidential Directive PDD-63 (1998) 3) Homeland Security Act (2002) 4) Federal Information Security Management Act (FISMA) 5) Cybersecurity Act of 2015 6) Federal Cybersecurity Workforce Assessment Act 7) Cybersecurity and Infrastructure Agency Act of 2018 8) State and Local Cybersecurity Act of 2019 Cyber Crime Statutes and Penalties			
T02		Reading and Analysis	Exam	CL01, CL03
T03	1) Statutes 2) Offenses and Penalties	Case Study Reviews	Case Studies	CL03
T04	Cybersecurity International and	Reading and Analysis	Exam	CL01, CL04

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
T05	Domestic Standards 1) International Standards 2) Domestic Standards Industry-Specific Regulations 1) Telecommunications Industry 2) Energy Industry 3) Healthcare Industry 4) Financial Industry 5) Federal Government 6) Education and Family Services Careers in Cybersecurity Law and Regulatory Compliance 1) Criminal Justice 2) Homeland Security 3) Defense and Defense Contracting	Reading and Analysis	Exam	CL01, CL04
T06	4) Federal, State and Local Government 5) IT/Corporate Security Office 6) Auditing and Accounting 7) Personnel and HR	Reading and Analysis	Exam, Final Project	CL01, CL02, CL04, CL05

12. Methods of Instruction

In the structuring of this course, what major methods of instruction will be utilized?

- o Class lecture
- o Discussion
- o Demonstrations
- o Programs and online presentations

13. General Education Goals Addressed by this Course (this section is to fulfill state requirements)

Information

Communication-Written and Oral

Quantitative Knowledge and Skills

Scientific Knowledge and Reasoning

Technological Competency

Yes

Related Course Learning Outcome

CL02, CL04

Related Outline Component

TO1, TO4

Assessment of General Education Goal (Recommended but not limited to)

Exam, Written Assignments, Projects and Presentations

Information Literacy

Society and Human Behavior

Humanistic Perspective

Historical Perspective

Global and Cultural Awareness

Ethical Reasoning and Action

Independent/Critical Thinking

Yes

Related Course Learning Outcome

CL02, CL03, CL05

Related Outline Component

TO2-TO4

Assessment of General Education Goal (Recommended but not limited to)

Exam, Written Assignments

14. Needs

Instructional Materials (text etc.):

Appropriate textbooks and/or Open Educational Resources will be selected. Class notes, presentations, software and online materials.

Technology Needs:

College Portal and/or College Distance Learning Platform and/or Textbook or Instructor Website.

Human Resource Needs (Presently Employed vs. New Faculty):

Presently Employed Faculty.

Facility Needs:

Classrooms equipped with computer workstations.

Library needs:

None.

15. Grade Determinants

The final grade in the course will be the cumulative grade based on the following letter grades or their numerical equivalents for the course assignments and examinations

A: Excellent

B+: Very Good

B: Good

C+: Above Average

C: Average

D: Below Average

F: Failure

I: Incomplete

R: Audit

For more detailed information on the Ocean County College grading system, please see Policy #5154.

Reviewer Comments