EXHIBIT B

OCEAN
COUNTY COLLEGE

BOARD OF TRUSTEES

Bylaw, Policy, and Curriculum Committee Agenda Items

To: Board of Trustees

From: Office of the President

Date: June 22, 2023

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, June 29, 2023**:

1. Recommend approval of the following new policies:

    a. Policy #2210, Administration, Administrative Operations, Data Information Security – Written Information Security Program **(Exhibit B-1)**
    b. Policy #2220, Administration, Administrative Operations, Data Classification **(Exhibit B-2)**

2. Recommend approval of the following items as accepted by the College Senate at its meeting on June 1, 2023:

    a. Revised policies:

        1) Policy #5152, Students, Academic Standards, Graduation **(Exhibit B-3)**
        2) Policy #7180, Educational Programs, Course and Curriculum, Experiential Learning **(Exhibit B-4)**

EXHIBIT B-1

Ocean County College, Toms River, NJ

ADMINISTATION
ADMINISTRATIVE OPERATIONS
Data Information Security –
<u>Written Information Security Program #2210</u>

<u>POLICY</u>

Ocean County College (OCC) is required by the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations (16 C.F.R. §§ 314), to implement and maintain a comprehensive Written Information Security Program (WISP).

Ocean County College shall develop and will implement, maintain, and update (as appropriate) a Written Information Security Program (WISP). The program shall follow the required elements as set forth in the Federal Student Aid (FSA)/Department of Education (DOE) Electronic Announcement ID: GENERAL-23-09, Subject: "Updates to the Gramm-Leach-Bliley Act (GLBA) Cybersecurity Requirements," Dated: February 9, 2023, and other related GLBA compliance guidance.

The "Senior Information Technology Leader" of the College is designated as the "Information Security Coordinator" of the WISP, along with the authority and responsibility for developing, implementing, coordinating, editing, maintaining, and otherwise executing the program.

The College shall design, develop, and implement, with Board approval, such policies and procedures necessary to ensure the timely and orderly enactment and execution of the Written Information Security Program.

If the WISP should conflict with any College policy or procedure, the provisions of the WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception.

The program is to be reviewed and updated periodically, but at least annually, along with a report to the Board of Trustees on any revisions to the program as well as activities performed against the program. Unless otherwise agreed upon by the Board, the program's annual report is to be presented during a June Board meeting.

ADOPTED: June 29, 2023
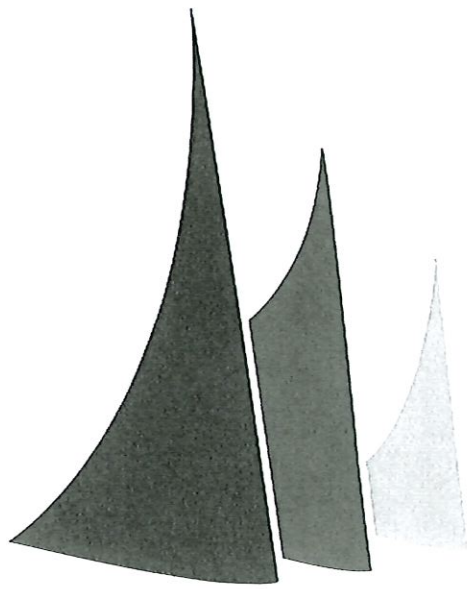
OCEAN
COUNTY COLLEGE

Information Security Program

June 29, 2023

Contents

Introduction

The objectives of this comprehensive Written Information Security Program (WISP) include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Ocean County College ("OCC" or "College" or "the College") has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule, 16 C.F.R. §§ 314.1 to 314.6, and other related Federal, State, and applicable laws.

If this WISP conflicts with any College policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3).

Section 1 – Purpose

The purpose of this WISP is to:

A. Ensure the security, confidentiality, integrity, and availability of personal [and other sensitive] information OCC collects, creates, uses, and maintains.
B. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
C. Protect against unauthorized access to or use of OCC-maintained personal [and other sensitive] information that could result in substantial harm or inconvenience to any customer or employee.

D. Define an Information Security Program that is appropriate to the College's size, scope, and business, its available resources, and the amount of personal [and other sensitive] information that OCC owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

Section 2 – Scope

This WISP applies to all employees, contractors, officers, and Board members of the College. It applies to any records that contain personal [or other sensitive] information in any format and on any media, whether in electronic or paper form.

A. For purposes of this WISP, "personal information" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:
   (i)   Social Security number;
   (ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;
   (iii) Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account (GLBA), or any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information, where personally identifiable financial information includes any information:
      a. A student/consumer provides OCC to obtain financial aid or other financial product or service;
      b. About a student/consumer resulting from any transaction involving financial aid or other financial product or service with OCC; or
      c. Information OCC otherwise obtains about a consumer in connection with providing financial aid or other financial product or service.
   (iv) Health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by OCC, which identifies or for which there is a reasonable basis to believe the information can be used to identify the individual and which relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual;
   (v)   Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;
   (vi) Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris; or
   (vii) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.
B. Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from Federal, State, or local government records.
C. For purposes of this WISP, "sensitive information" means data that:
   (i)   The College considers to be highly confidential information; or
   (ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to the College, its students, customers, or business partners.

(iii) Sensitive information includes, but is not limited to, personal information. [See OCC's information classification policy, available in Policy #   .

Section 3 – Information Security Coordinator

Ocean County College has designated the Senior Information Technology Leader of the College (the "Information Security Coordinator") to implement, coordinate, and maintain this WISP. The Information Security Coordinator shall be responsible for:

A. Initial implementation of this WISP, including:
   (i) Assessing internal and external risks to personal [and other sensitive] information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);
   (ii) Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);
   (iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal [and other sensitive] information (see Section 6);
   (iv) Ensuring that the safeguards are implemented and maintained to protect personal [and other sensitive] information throughout OCC, where applicable (see Section 6);
   (v) Overseeing service providers that access or maintain personal [and other sensitive] information on behalf of the College (see Section 7);
   (vi) Monitoring and testing the Information Security Program's implementation and effectiveness on an ongoing basis (see Section 8);
   (vii) Defining and managing incident response procedures (see Section 9); and
   (viii)   Establishing and managing enforcement policies and procedures for this WISP, in collaboration with College human resources and management (see Section 10).
B. Engaging qualified information security personnel, including:
   (i) Providing them with security updates and training sufficient to address relevant risks; and
   (ii) Verifying that they take steps to maintain current information security knowledge.
C. Employee, contractor, and (as applicable) stakeholder training, including:
   (i) Providing periodic training regarding this WISP, OCC's safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal [or other sensitive] information, updated as necessary or indicated by OCC's risk assessment activities (see Section 4);
   (ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through the OCC training portal; and
   (iii) The Human Resources Department is responsible for retaining training and acknowledgment records.
D. Reviewing this WISP and the security measures defined here at least annually, when indicated by OCC's risk assessment (see Section 4) or program monitoring and testing activities (see Section 8), or whenever there is a material change in OCC's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information (see Section 11).
E. Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or OCC's information security policies and procedures.
F. Periodically, but at least annually, reporting to OCC's Board of Trustees [in writing] regarding the status of the Information Security Program and OCC's safeguards to protect personal [and other sensitive]

information[, including the program's overall status, compliance with applicable laws and regulations, material matters related to the program, such as risk assessment, risk management and control decisions, service provider arrangements, testing results, cyber incidents or policy violations and management's responses, and recommendations for program changes].

Section 4 – Risk Assessment

As a part of developing and implementing this WISP, the College will conduct and base its Information Security Program on a periodic, documented risk assessment, at least annually, or whenever there is a material change in OCC's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information.

A. The risk assessment shall:
  (i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal [or other sensitive] information and include criteria for evaluating and categorizing those identified risks;
  (ii) Define assessment criteria and assess the likelihood and potential damage that could result from such risks, including the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the personal [or other sensitive] information, taking into consideration the sensitivity of the personal [and other sensitive] information; and
  (iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:
    a. Employee, contractor, and (as applicable) stakeholder training and management;
    b. Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures;
    c. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
    d. OCC's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.
B. Following each risk assessment, Ocean County College will:
  (i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
  (ii) Reasonably and appropriately address any identified gaps, including documenting OCC's plan to remediate, mitigate, accept, or transfer identified risks, as appropriate; and
  (iii) Regularly monitor the effectiveness of OCC's safeguards, as specified in this WISP (see Section 8).

Section 5 – Information Security Policies and Procedures

As part of this WISP, the College will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

A. Establish policies regarding:
  (i) Information classification;
  (ii) Information handling practices for personal [and other sensitive] information, including the storage, access, disposal, and external transfer or transportation of personal [and other sensitive] information;

(iii) User access management, including identification and authentication (using passwords or other appropriate means);

(iv) Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD); and

(ix) Information systems acquisition, development, operations, and maintenance.

B. Detail the implementation and maintenance of OCC's administrative, technical, and physical safeguards (see Section 6).

Section 6 – Safeguards

The College will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal [or other sensitive] information that OCC owns or maintains on behalf of others.

A. Safeguards shall be appropriate to OCC's size, scope, and business, its available resources, and the amount of personal [and other sensitive] information that the College owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

B. OCC shall document its administrative, technical, and physical safeguards in OCC's information security policies and procedures (see Section 5).

C. OCC's safeguards shall, at a minimum include:

(i) Implementing and periodically reviewing technical and, as appropriate, physical access controls to:

    a. Authenticate and permit access to personal [and other sensitive] information only to authorized users; and

    b. Limit authorized users' access only to personal [and other sensitive] information that they need to perform their duties and functions, or in the case of customers, to access their own personal information;

(ii) Identifying and managing the data, personnel, devices, systems, and facilities that enable the College to achieve its business purposes according to business priorities, objectives, and OCC's risk management strategy;

(iii) Encrypting personal [and other sensitive] information that OCC holds when it is at rest or in transit over external networks, unless the College determines that applying encryption is currently infeasible for its circumstances and the Information Security Coordinator reviews and approves effective compensating controls under OCC's exceptions process (see Section 3(e));

(iv) Adopting secure development practices for the in-house developed applications and procedures for evaluating, assessing, or testing the security of externally developed applications that in either case the College uses to transmit, access, or store personal [or other sensitive] information;

(v) Implementing multifactor authentication for individuals accessing personal [or other sensitive] information or systems that handle personal [or other sensitive] information unless the Information Security Coordinator reviews and approves the use of reasonably equivalent or more secure controls under OCC's exceptions process (see Section 3(e));

(vi) Developing, implementing, and maintaining procedures for securely disposing of personal [and other sensitive] information in any format, including:

a. Disposing of customers' personal information, no later than two years after the last date the College uses it for provisioning a product or service to the relevant customer unless it is necessary for business operations or other legitimate business purposes, retention is otherwise required by law, or targeted disposal is not reasonably feasible due to the way the College maintains it; and

b. Periodically reviewing data retention policies to minimize the unnecessary retention of personal [and other sensitive] information.

(vii) Adopting change management procedures;

(viii) Implementing policies, procedures, and controls to monitor and log authorized users' activities and detect unauthorized access to, use of, or tampering with personal [or other sensitive] information by them.

Section 7 – Service Provider Oversight

Ocean County College will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal [or other sensitive] information on its behalf by:

A. Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and OCC's obligations.

B. Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and OCC's obligations.

C. Monitoring and periodically auditing the service provider's performance to verify compliance with this WISP and all applicable laws and OCC's obligations.

Section 8 – Monitoring

Ocean County College will regularly test and monitor the implementation and effectiveness of its Information Security Program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal [or other sensitive] information. The College shall reasonably and appropriately address any identified gaps. GLBA: OCC's testing and monitoring program shall address the effectiveness of OCC's safeguards, specifically their key controls, systems, and procedures, including those the College uses to detect attempted and actual attacks on or intrusions into its networks and systems that handle personal [or other sensitive] information. Specifically, OCC will implement and maintain as appropriate for its networks and systems that handle personal [or other sensitive] information either:

A. Continuous monitoring or other systems to detect on an ongoing basis changes that may create vulnerabilities; or

B. A combination of the following according to OCC's risk assessment (see Section 4):
   (i) Annual penetration testing; and
   (ii) Periodic vulnerability assessments, including scans or reviews reasonably designed to identify publicly known security vulnerabilities, conducted at least every six months and whenever there are material changes to OCC's operations or business arrangements or circumstances occur that may have a material impact on OCC's information security program.

Section 9 – Incident Response

Ocean County College will establish and maintain written policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

A. Defining:
   (i) The incident response plan's goals;
   (ii) OCC's incident response processes;
   (iii) Roles, responsibilities, and levels of decision-making authority; and
   (iv) Processes for internal and external communications and information sharing.
B. Identifying remediation requirements to address any identified weaknesses in OCC's systems and controls.
C. Documenting and appropriately reporting information security incidents and OCC's response activities
D. Performing post-incident reviews and updating the plan as appropriate.

Section 10 – Enforcement

Violations of this WISP may result in disciplinary action, in accordance with OCC's policies and procedures, collective bargaining agreements, and employee handbooks. OCC's progressive disciplinary processes are detailed in collective bargaining agreements for represented employees and employee handbooks for non-represented employees.

Section 11 – Program Review

Ocean County College will review this WISP and the security measures defined herein at least annually, when indicated by OCC's risk assessment (see Section 4) or program monitoring and testing activities (see Section 8), or whenever there is a material change in OCC's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information.

A. The College shall retain documentation regarding any such program review, including any identified gaps and action plans.

Effective Date

This WISP is effective upon Board approval.

ADOPTED: June 29, 2023

EXHIBIT B-2

Ocean County College, Toms River, NJ   ADMINISTATION
                                                         ADMINISTRATIVE OPERATIONS
                                                         <u>Data Classification #2220</u>

<u>Policy</u>

Any person who uses, stores, or accesses data contained in the information technology systems (either academic or administrative) of Ocean County College has the responsibility to safeguard that data. Data classification is one method of determining the safeguard requirements for certain data and the appropriate College response to any unauthorized release of that data. Such safeguards and response plans are not only good stewardship for College data, but are required by certain state and federal law and regulations.

This policy governs the privacy, security, and integrity of College data stored on College IT systems and outlines the responsibilities of the individuals and organizational units that manage, use, access, store, or transmit that data. This policy supplements, but does not supersede, the College's Confidentiality Agreement.

I.   Ocean College IT Services maintains systems that store data essential to the performance of College business. All members of the College community have a responsibility to protect College data from unauthorized access, use, storage, transmission, disclosure, or destruction.

II.   All College data is classified into four levels of security: Restricted (Protected) Data, Confidential (Sensitive) Data, Internal (Directory) Data, and Public Data. For the purposes of this policy, data not formally classified (Unclassified Data) will be considered Sensitive Data. For the purposes of the College's Confidentiality Agreement, all data except Public Data is to be considered confidential.

       a.   Restricted or Protected Data is data that (1) if compromised would expose members of the College and its community to a high risk of identity theft or financial fraud and (2) is protected by Federal or state law or regulations. Applicable law and regulatory requirements include (but are not limited to) the Family Educational Rights and Privacy Act (FERPA), the Fair and Accurate Credit Transactions Act (FACTA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and other applicable Federal and New Jersey State laws. Examples of Protected Data include, but are not limited to:
            i.   Social Security number
            ii.   Driver's license number, Passport Number, or any State ID Number
            iii. Credit card information (Number, expiration date, security code)
            iv.   Date of birth
            v.   Users' systems passwords
            vi.   Medical history
            vii. Disability
            viii. Student and family financial history
            ix.   Student account balances

  x. Student Financial Aid history

  xi. Student academic history, including student grades

b. Confidential or Sensitive Data is data that, while not explicitly protected by Federal or State law, is proprietary to the College and would, if released, expose the College and members of the community to a heightened risk of identity theft or financial fraud. Examples of Sensitive Data include, but are not limited to:

  i. Employee salary or employment history

  ii. Permanent or local address

  iii. Department budgets

  iv. Student registration Personal Identification Numbers

  v. Internal operating procedures and operational manuals

  vi. Internal memoranda, emails, reports, and other documents

  vii. Technical documents, such as system configurations and floor plans

c. Internal or Directory Data is data that the College chooses to keep private, but any disclosure would most likely not cause material harm. It can also be used for College communication or to link records between College systems or reports. This could include directory information that is widely available to members of the College community, but nevertheless should be handled with care, since exposure could result in increased risk of financial fraud or identity theft for the College and members of the community. Examples of Internal/Directory Data include, but are not limited to:

  i. Departmental policies and procedures

  ii. Grant applications

  iii. Usernames

  iv. Campus wide IDs

  v. ID photos

  vi. Class rosters/Advisor rosters

d. Public Data is data that the College may or must make available to the public with no legal or other restrictions, via its website or various reports, press releases, and the like. Examples of Public Data include:

  i. Information posted on the College's website

  ii. The College phone directory

  iii. The College's annual financial reports

  iv. Data published in the Integrated Postsecondary Education Data System documents

  v. Copyrighted materials that are publicly available

e. When in doubt as to how any data should be classified among the four levels of security classifications above, contact your supervisor.

III. The loss, unauthorized access to, or disclosure of Protected Data must be reported to the appropriate College officials, including the management of the organizational unit in which the data breach was discovered, the College's Chief Information Officer (CIO), and the Technology Helpdesk so that the appropriate response to the incident, including required notification of appropriate Federal and State agencies, can be initiated.

IV.   The loss, unauthorized access to, or disclosure of Sensitive Data should be reported to the management of the organizational unit in which the data breach was discovered for its appropriate response.

V.   For the purposes of the College's Confidentiality Agreement, all data except Public Data are considered confidential. The unauthorized access, disclosure, or transmission of confidential information may result in disciplinary action by the College, including termination or expulsion, as outlined in the College's Confidentiality Agreement and other relevant College policies.

VI.   College data are assets belonging to the College. Departments which collect, use, store, and transmit College data should classify their data according to the level of risk associated with handling that data and implement appropriate safeguards to that data based on that risk. Data are generally stored in sets. The classification of a data set should be to the highest level of any data element in that set; for example, a report containing a combination of protected, sensitive directory and public data should be considered protected and provided with the safeguards appropriate for protected data. Individuals and departments must implement appropriate safeguards for accessing, transmitting, and storing College data. Examples of appropriate safeguards for Protected and Sensitive Data include, but are not limited to:

   a.   The data must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
   b.   The data may only be accessed or disclosed if necessary for College business purposes and consistent with applicable College policies.
   c.   The data must not be downloaded, stored, or transmitted unless appropriately secured and/or encrypted.
   d.   The data must not be posted on any website or shared file storage space unless College standard authentication methods are used.
   e.   The data must be destroyed when no longer needed and in accordance with College policies.

An Information Security Classification Reference Guide is attached to this policy to assist in identifying data classification.

ADOPTED: June 23, 2023

Information Security Classification Reference Guide – June 29, 2023

Public Use Data Intended for release to the public	Internal/Directory Data May be shared only within the OCC community	Confidential/Sensitive Data Intended only for those with a "business need to know"	Restricted/Protected Data Requires strict controls
The College intentionally provides this information to the public.	The College chooses to keep this information private, but any disclosure would not cause material harm.	Disclosure of this information beyond the intended recipients may cause harm to the individual and/or the College.	Disclosure of this information beyond the specified recipients would likely cause serious harm to the individual and/or the College.
Examples: • Public phone directories • Student directory information* • Marketing materials • Course catalogs • Annual reports • Press releases • Regulatory and legal filings *Directory information about students who have requested FERPA blocks must be classified and handled as Confidential/Sensitive data.	**Examples:** • Departmental policies and procedures • Grant applications • Physical plant information that is not confidential or restricted • Non-public building plans or layouts that are not confidential or restricted • Campus wide IDs • ID photos • Class Rosters/Advisor Rosters	**Examples:** • Non-directory student information • Information protected under FERPA • Personnel Records • Donor information • Budget/financial transactions • Internal operating procedures and operational manuals • Internal memoranda, emails, reports and other documents • Technical documents such as system configurations and floor plans	**Examples:** • Government issued identifiers such as Social Security Number, Passport number, Driver's License Number, or any State ID Number • Individually identifiable financial account information such as Bank accounts, Credit/Debit Card information (number, expiration date, security code) • Personally Identifiable Information (PII) • User System Passwords/PINs • Individually identifiable health or medical/disability information • Student and family Financial/Financial Aid history, account balances, etc.

Feedback: If you have questions or concerns about the policy, or if you know of items that are out of compliance, please contact your supervisor or the College Chief Information Officer (CIO).

Use Your Good Judgement: The lists above are only examples and are not definitive classifications. When in doubt as to how any data should be classified among the four levels of security classification, contact your supervisor.

EXHIBIT B-3

POLICY

1. To qualify as a candidate for the degree of Associate in Arts, Associate in Science, or Associate in Applied Science, a student must have the following:

    a. A minimum of 60 hours of non-remedial credit which must include all courses required in the curriculum elected by the student.

    Minimum requirements as indicated below:

    ### Associate in Arts Degree

9 cr.	Communication
3~~6~~ cr.	History
6~~9~~ cr.	Humanities
6 cr.	Social Science
3 cr.	Diversity [This requirement cannot be satisfied by the same course used to satisfy the categories above.]
6~~12~~ cr.	Mathematics (3-4~~3~~-8 cr.) / Science (3-4-8 cr.) / Technology (0~~)-4~~ cr.)

    Students must select one math course and~~,~~ one lab science course.~~, and one technology course, and must complete the 12 cr. requirement with any additional math or science course from the current List of Approved General Education Courses. Students may attempt to "test out" of the technology requirement. If they succeed, they must take additional credits in math or science from the List of Approved General Education Courses.~~

27~~15~~ cr.	Elective Courses (can include any additional necessary General Education courses)
60 cr.	**TOTAL CREDITS (33~~45~~ General Education Credits)**

    ### Associate in Science Degree

6 cr.	Communication
3 cr.	Humanities
3 cr.	Social Science
3 cr.	Additional Humanities or Social Science
9 cr.	Mathematics (3-8 cr.) / Science (3-8 cr.) / Technology (0-4 cr.)

    Students must select one math course, one lab science course, and one technology course from the current List of Approved General Education Courses. Students may attempt to "test out" of the technology requirement. If they succeed, they must take additional credits in math or science from the List of Approved General Education Courses.

6 cr.	Additional General Education Credit [from the categories above]
18 cr.	Department Concentration / Program Specific Requirements
12 cr.	Elective Courses
60 cr.	**TOTAL CREDITS (30 General Education Credits)**

<u>Associate in Applied Science Degree</u>

6 cr.	Communication
3 cr.	Humanities or Social Science
3 cr.	Mathematics – Science – Technology
	Students must select any math, science, or technology course from the current List of Approved General Education Courses.
8 cr.	Additional General Education Credit [from the categories above]
37 cr.	Program Specific Requirements
<u>3 cr.</u>	Elective Courses
<u>60 cr.</u>	**TOTAL CREDITS (20 General Education Credits)**

    b.   Waiver of courses requires that an equivalent number of credits must be completed to meet graduation requirements.

2. To qualify as a candidate for an Associate degree, a student must have earned at least 60 semester hours of non-remedial credit, or as specified otherwise for certain curricula, and accrued sufficient grade points for a cumulative grade point average of 2.00 (average grade of "C").

3.   a.   A student may transfer a maximum of 30 credit hours at any time during the student's candidacy for a degree.

    b.   Service personnel on active duty and their dependents must meet all College degree requirements with the following exceptions:

    (1)   A minimum of 24 semester hours of the 60 required must be earned through attendance of classes at Ocean County College.

    (2)   These 24 semester hours may be earned at any time during the student's candidacy for a degree.

4. The College will confer Associates degrees three times per year. Candidates for graduation must file an application for Graduation by an established deadline to be eligible for the next upcoming graduation. The specific deadlines and the actual dates of graduation will be determined by the Registrar, within the following guidelines:

- After the Fall Semester
  - deadline to apply: mid November
  - actual graduation: second week of January

- After the Spring Semester
  - deadline to apply: mid March
  - actual graduation: day of Commencement Ceremony

- After the Summer Sessions

- o   deadline to apply: mid July
- o   actual graduation day: last business day of August

5.   A candidate whose final cumulative grade point average is 3.50 or higher will be graduated with honors based on the following:

   3.50 - 3.79 cum laude (with honors)
   3.80 - 3.89 magna cum laude (with high honors)
   3.90 - 4.00 summa cum laude (with highest honors)

   A student graduating with honors will receive an emblem on the diploma, indicating the honors category. The appropriate honors distinction shall also be shown on the student's official College transcript.

6.   All specific courses required for a second degree must be completed without repeating any previous courses in which credit was earned. Neither will any courses judged to be at a lower academic level than those previously completed be used toward the second degree.

7.   No less than 18 additional credit hours, including those required, must be earned beyond the number established for the initial degree.

8.   The prescribed procedure will be followed in filing an application for a second degree.

9.   Additional degrees beyond the second normally will not be granted. Exceptions must be approved by the Academic Standards Committee.

ADOPTED: August 26, 1968
Revised: December 21, 1970
Revised: January 24, 1972
Revised: December 18, 1972
Revised: March 26, 1973
Revised: June 25, 1973
Revised: February 25, 1974
Revised: June 24, 1974
Revised: December 18, 1976
Revised: June 27, 1977
Revised: September 17, 1979
Revised: January 26, 1981
Revised: January 28, 1991
Revised: March 22, 1993
Revised: August 25, 2008
Revised: August 24, 2009
Revised: April 26, 2010

Revised: February 25, 2013
Revised: January 27, 2014
Revised: April 28, 2014
Revised: November 2, 2017
Revised: February 28, 2019
Revised: February 2023 (TBD)

EXHIBIT B-4

Ocean County College, Toms River, NJ

CURRICULUM

POLICY

The College shall establish an Experiential Learning program of internships, externships, and/or apprenticeships designed to provide students with the opportunity to explore and enhance their academic and career goals. Programs may or may not include the opportunity to earn college credit that may or may not be applicable to their degree program. Select experiential learning opportunities may involve paid positions.

The college will endeavor to ensure that all workplace agreements for the referral, assignment, and placement of students contain a non-discriminatory assurance from all participating employers (internal and external) stating they do not discriminate on the basis of race, color, national origin, sex or disability.

Definitions

- Internship: A semester-long work experience for college credit.
- Externship: A short job shadowing experience for zero college credit.
- Apprenticeship: A voluntary arrangement between an employer (sponsor) and employee (apprentice), which provides on-the-job training and classroom instruction.

ADOPTED: May 26, 1987
Revised: May 28, 2020

REVIEWED: November 5, 1991