Ocean County College, Toms River, NJ

ADMINISTRATION
ADMINISTRATIVE OPERATIONS
Data Information Security –
Written Information Security Program #2210

POLICY

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 #2220.

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