Rowan College
of South Jersey

Administrative Procedure: 8109.1
NONPUBLIC PERSONAL INFORMATION SECURITY

The Gramm-Leach-Bliley Act ("GLBA"), also known as the Financial Services Modernization Act of 1999, mandates that financial institutions, including colleges and universities, protect the privacy and security of customers' nonpublic personal information ("NPI"). Rowan College of South Jersey ("College") is committed to protecting the privacy and security of NPI and to complying with GLBA. By implementing this administrative procedure, the College aims to safeguard sensitive information and maintain the trust of its students, faculty, staff, and other stakeholders.

This administrative procedure establishes guidelines for complying with GLBA by protecting and safeguarding the privacy and security of NPI of students, faculty, staff, contractors, and third-party service providers who have access to or handle NPI. NPI protection covers all forms whether electronic, paper, or any other format. The goal is to prevent the unauthorized access, use, or disclosure of NPI and to ensure compliance with the GLBA.

Statements of Assurance

1. NPI refers to any information that is <u>not</u> publicly available and can be used to identify an individual. Examples of NPI include, but not limited to:

    - Social Security numbers;
    - Driver's Licenses;
    - Financial account numbers;
    - Credit card information;
    - Birthdates;
    - Contact information (e.g. addresses, phone numbers); and
    - Academic records.

2. The College will designate an employee as GLBA Compliance Officer who will be responsible for:

    - Overseeing implementation of this administrative procedure and guidelines;
    - Enforcement of this administrative procedure and guidelines;
    - Investigate and address any violations of this administrative procedure;

- Ensure appropriate measures are in place to protect NPI;
- Compliance with GLBA requirements; and
- Coordination annually of the review, revision, and update process of this administrative procedure.

3. The College will conduct a thorough and regular risk assessment to identify potential risks and vulnerabilities to the security and confidentiality of NPI. The risk assessment will include:

    - Identification of potential internal and external threats;
    - Evaluation of the effectiveness of existing security controls; and
    - Assessment of potential impacts of security breaches.

4. The College will establish and maintain a comprehensive information security program to protect NPI. The program will include administrative, technical, and physical safeguards designed to:

    - Ensure the security and confidentiality of NPI;
    - Protect against anticipated threats or hazards; and
    - Prevent unauthorized access, use, or disclosure of NPI.

5. The College will provide regular training and awareness programs for all employees, emphasizing the importance of protecting NPI and the responsibilities of each member of the College community. Training will include:

    - Understanding the GLBA and its requirements;
    - Recognizing and reporting security incidents; and
    - Implementing best practices for data protection.

6. The College will implement strict access control measures, including:

    - Restricting access to authorized individuals who require it to perform job functions;
    - Requiring user authentication and authorization; and
    - Reviewing access privileges regularly.

7. The College will ensure that third-party service providers with access to NPI include in their contracts:

    - Appropriate security measures to protect NPI;
    - Provisions for compliance with GLBA requirements; and
    - Regular security assessments.

8. The College will establish an incident response plan to address and mitigate security breaches involving NPI to include:

- Identification and containment of the breach;
- Notification procedures for affected individuals;
- Investigation and documentation of the breach;
- Corrective action to prevent future incidents; and
- Informing the U.S. Department of Education via the Cybersecurity Breach Intake form.

All members of the College community are expected to comply with this administrative procedure. Violations of this administrative procedure may result in disciplinary action, up to and including expulsion from the College or termination of employment.

This administrative procedure will be reviewed annually and updated as necessary to ensure compliance with the GLBA and address emerging security threats and vulnerabilities.

Area: Student Services
Approved: 02/18/25

President's Authorization: 

References:

Rowan College of South Jersey Board of Trustees Policy Manual, *8109 Student Records*

Gramm-Leach-Bliley Act (GLBA) U.S.C. 15 U.S.C. §§ 6801-6809 and C.F.R. 16 C.F.R. pts. 313-314