[First Reprint]

ASSEMBLY, No. 817

STATE OF NEW JERSEY

221st LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2024 SESSION

Sponsored by:
Assemblyman GREGORY P. MCGUCKIN
District 10 (Monmouth and Ocean)
Assemblyman PAUL KANITRA
District 10 (Monmouth and Ocean)
Assemblywoman TENNILLE R. MCCOY
District 14 (Mercer and Middlesex)

Co-Sponsored by:
Assemblyman Scharfenberger, Assemblywomen Flynn, Speight and Bagolie

SYNOPSIS

Requires public institution of higher education to establish plans concerning cyber security and prevention of cyber attacks.

CURRENT VERSION OF TEXT

As reported by the Assembly Higher Education Committee on February 22, 2024, with amendments.

(Sponsorship Updated As Of: 3/18/2024)

AN ACT concerning higher education cyber security and supplementing Title 18A of the New Jersey Statutes.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

[1]1. As used in this act:

"Cyber attack" means unauthorized access to electronic files, media, or data containing personal information that compromises the security, confidentiality, or integrity of personal information when access to the personal information has not been secured by encryption or any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the public institution of higher education for a legitimate purpose, or for a purpose authorized under State or federal law, shall not constitute a cyber attack, provided that the personal information is not used for a purpose unrelated to the public institution of higher education or subject to further unauthorized disclosure.

"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements:

(1) Social Security number;

(2) driver's license number or State non-driver identification card number;

(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(4) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account, including an account issued by a public institution of higher education.

Personal information shall not include publicly available information that is lawfully made available to the general public from federal, State, or local government records, or widely distributed media. Personal information shall include dissociated data that, if linked, would constitute personal information, if the means to link the dissociated data were accessed in connection with access to the dissociated data.

"Phishing" means attempts to fraudulently acquire an individual's personal information by masquerading as a trustworthy business or entity by means of a web page, electronic mail message,

EXPLANATION – Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.
Matter enclosed in superscript numerals has been adopted as follows:
[1]Assembly AHI committee amendments adopted February 22, 2024.

or otherwise through the use of the Internet to solicit, request, or take any action to induce another person to provide personal information by representing oneself, either directly or by implication, to be a business or entity without the authority or approval of that business or entity.[1]

[1]**[**1.**]** 2.[1] a. A public institution of higher education shall establish plans and procedures to enhance cyber security and prevent cyber attacks against the institution's information technology systems. The plans and procedures, at a minimum, shall address: system monitoring to identify potential cyber security risks and vulnerabilities; cyber threat assessment; techniques for mitigating risk and preventing cyber breaches; and response and recovery for cyber security incidents.

b. In developing its cyber security plans and procedures, an institution of higher education may consult with the New Jersey Cybersecurity and Communications Integration Cell, established pursuant to Executive Order No. 178 (2015) in the New Jersey Office of Homeland Security and Preparedness, regarding information and best practices on cyber security and data protection.

c. A public institution of higher education shall, as appropriate and on a regular basis, update its cyber security plans and procedures to reflect current technologies and information security techniques.

d. A public institution of higher education shall notify the New Jersey Office of Homeland Security and Preparedness of any cyber attack against the institution's information technology systems [1]**[**within 24 hours of becoming aware of the incident**]** in a manner consistent with the provisions of P.L.2023, c.19 (C.52:17B-193.2 et seq.). A phishing attempt shall not be considered a cyber attack for the purposes of this subsection[1].

[1]**[**2.**]** 3.[1] This act shall take effect immediately.