

[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:

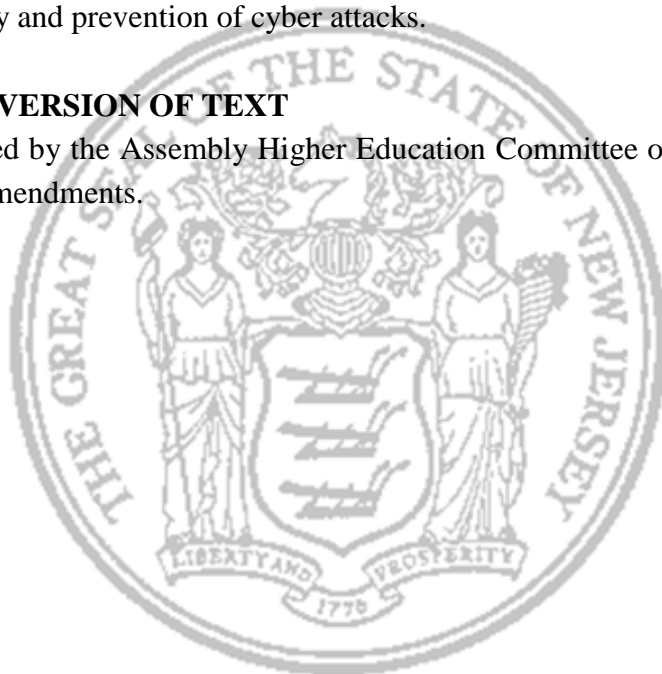
Assemblyman Scharfenberger, Assemblywomen Flynn, Speight and Bagolie

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)

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

3

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

6

7 ¹1. As used in this act:

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

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

23 (1) Social Security number;

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

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

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

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

42 “Phishing” means attempts to fraudulently acquire an
43 individual’s personal information by masquerading as a trustworthy
44 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:

¹Assembly AHI committee amendments adopted February 22, 2024.

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

6
7 ¹**[1.]** 2.¹ a. A public institution of higher education shall
8 establish plans and procedures to enhance cyber security and
9 prevent cyber attacks against the institution's information
10 technology systems. The plans and procedures, at a minimum, shall
11 address: system monitoring to identify potential cyber security risks
12 and vulnerabilities; cyber threat assessment; techniques for
13 mitigating risk and preventing cyber breaches; and response and
14 recovery for cyber security incidents.

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

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

26 d. A public institution of higher education shall notify the New
27 Jersey Office of Homeland Security and Preparedness of any cyber
28 attack against the institution's information technology systems
29 ¹**[within 24 hours of becoming aware of the incident]** in a manner
30 consistent with the provisions of P.L.2023, c.19 (C.52:17B-193.2 et
31 seq.). A phishing attempt shall not be considered a cyber attack for
32 the purposes of this subsection¹.

33
34 ¹**[2.]** 3.¹ This act shall take effect immediately.