

# HOUSE BILL 1122

P1, F2

0lr2299  
CF SB 588

---

By: **Delegates Pena–Melnik, B. Barnes, Lehman, and Williams**

Introduced and read first time: February 6, 2020

Assigned to: Appropriations

---

## A BILL ENTITLED

1 AN ACT concerning

2 **State Government – Protection of Personally Identifiable Information –**  
3 **University System of Maryland**

4 FOR the purpose of excluding the University System of Maryland from certain provisions  
5 of law governing protection of information by government agencies; requiring the  
6 University System of Maryland to review and designate certain systems as systems  
7 of record based on certain criteria; requiring the University to develop and adopt a  
8 certain privacy governance program to govern each system of record; requiring the  
9 University to develop and adopt a certain information security and risk management  
10 program for the protection of personally identifiable information; requiring the  
11 University to publish a certain privacy notice on the University’s website; requiring  
12 the notice to include certain information; requiring the University, when destroying  
13 certain records, to take certain steps to protect against unauthorized access to or use  
14 of personally identifiable information; requiring the University, if it discovers or is  
15 notified of a breach of the security of a system, to conduct a certain investigation and,  
16 if the University determines that a certain breach has occurred, provide certain  
17 notices to certain individuals in a certain manner; establishing that this Act does not  
18 apply to certain personally identifiable information; establishing that compliance  
19 with certain provisions of law does not authorize the University to fail to comply with  
20 certain other provisions of law; defining certain terms; altering a certain definition;  
21 providing for a delayed effective date; and generally relating to protection of  
22 personally identifiable information by the University System of Maryland.

23 BY repealing and reenacting, without amendments,  
24 Article – State Government  
25 Section 10–1301(a)  
26 Annotated Code of Maryland  
27 (2014 Replacement Volume and 2019 Supplement)

28 BY repealing and reenacting, with amendments,  
29 Article – State Government

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 Section 10–1301(f)  
2 Annotated Code of Maryland  
3 (2014 Replacement Volume and 2019 Supplement)

4 BY adding to  
5 Article – State Government  
6 Section 10–13A–01 through 10–13A–04 to be under the new subtitle “Subtitle 13A.  
7 Protection of Personally Identifiable Information by the University System of  
8 Maryland”  
9 Annotated Code of Maryland  
10 (2014 Replacement Volume and 2019 Supplement)

11 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,  
12 That the Laws of Maryland read as follows:

13 **Article – State Government**

14 10–1301.

15 (a) In this subtitle the following words have the meanings indicated.

16 (f) **(1)** “Unit” means:

17 **[(1)] (I)** an executive agency, or a department, a board, a commission, an  
18 authority, a public institution of higher education **OTHER THAN THE UNIVERSITY**  
19 **SYSTEM OF MARYLAND**, a unit, or an instrumentality of the State; or

20 **[(2)] (II)** a county, municipality, bi–county, regional, or multicounty  
21 agency, county board of education, public corporation or authority, or any other political  
22 subdivision of the State.

23 **(2) “UNIT” DOES NOT INCLUDE THE UNIVERSITY SYSTEM OF**  
24 **MARYLAND.**

25 **SUBTITLE 13A. PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION BY**  
26 **THE UNIVERSITY SYSTEM OF MARYLAND.**

27 **10–13A–01.**

28 **(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS**  
29 **INDICATED.**

30 **(B) (1) “BREACH OF THE SECURITY OF A SYSTEM” MEANS THE**  
31 **UNAUTHORIZED ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION**  
32 **MAINTAINED BY THE UNIVERSITY SYSTEM OF MARYLAND THAT CREATES A**

1 REASONABLE RISK OF HARM TO THE INDIVIDUAL WHOSE PERSONALLY  
2 IDENTIFIABLE INFORMATION WAS SUBJECT TO UNAUTHORIZED ACQUISITION.

3 (2) "BREACH OF THE SECURITY OF A SYSTEM" DOES NOT INCLUDE:

4 (I) THE GOOD FAITH ACQUISITION OF PERSONALLY  
5 IDENTIFIABLE INFORMATION BY AN EMPLOYEE OR AGENT OF THE UNIVERSITY  
6 SYSTEM OF MARYLAND FOR THE PURPOSES OF THE UNIVERSITY, PROVIDED THAT  
7 THE PERSONALLY IDENTIFIABLE INFORMATION IS NOT USED OR SUBJECT TO  
8 FURTHER UNAUTHORIZED DISCLOSURE; OR

9 (II) PERSONALLY IDENTIFIABLE INFORMATION THAT WAS  
10 SECURED BY ENCRYPTION OR REDACTED AND FOR WHICH THE ENCRYPTION KEY  
11 HAS NOT BEEN COMPROMISED OR DISCLOSED.

12 (C) "ENCRYPTION" MEANS THE PROTECTION OF DATA IN ELECTRONIC OR  
13 OPTICAL FORM, IN STORAGE OR IN TRANSIT, USING A TECHNOLOGY THAT:

14 (1) IS CERTIFIED TO MEET OR EXCEED THE LEVEL THAT HAS BEEN  
15 ADOPTED BY THE FEDERAL INFORMATION PROCESSING STANDARDS ISSUED BY  
16 THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; AND

17 (2) RENDERS SUCH DATA INDECIPHERABLE WITHOUT AN  
18 ASSOCIATED CRYPTOGRAPHIC KEY NECESSARY TO ENABLE DECRYPTION OF SUCH  
19 DATA.

20 (D) "INDIVIDUAL" MEANS A NATURAL PERSON.

21 (E) "LEGITIMATE BASIS" MEANS THE UNIVERSITY SYSTEM OF MARYLAND  
22 HAS A CONTRACTUAL NEED, PUBLIC INTEREST PURPOSE, BUSINESS PURPOSE, OR  
23 LEGAL OBLIGATION FOR PROCESSING OR THAT THE INDIVIDUAL HAS CONSENTED  
24 TO THE UNIVERSITY'S PROCESSING OF THE INDIVIDUAL'S PERSONALLY  
25 IDENTIFIABLE INFORMATION.

26 (F) (1) "PERSONALLY IDENTIFIABLE INFORMATION" MEANS ANY  
27 INFORMATION THAT, TAKEN ALONE OR IN COMBINATION WITH OTHER  
28 INFORMATION, ENABLES THE IDENTIFICATION OF AN INDIVIDUAL, INCLUDING:

29 (I) A FULL NAME;

30 (II) A SOCIAL SECURITY NUMBER;

31 (III) A DRIVER'S LICENSE NUMBER, STATE IDENTIFICATION

1 CARD NUMBER, OR OTHER INDIVIDUAL IDENTIFICATION NUMBER;

2 (IV) A PASSPORT NUMBER;

3 (V) BIOMETRIC INFORMATION INCLUDING AN INDIVIDUAL'S  
4 PHYSIOLOGICAL, BIOLOGICAL, OR BEHAVIORAL CHARACTERISTICS, INCLUDING AN  
5 INDIVIDUAL'S DEOXYRIBONUCLEIC ACID (DNA), THAT CAN BE USED, SINGLY OR IN  
6 COMBINATION WITH EACH OTHER OR WITH OTHER IDENTIFYING DATA, TO  
7 ESTABLISH INDIVIDUAL IDENTITY;

8 (VI) GEOLOCATION DATA;

9 (VII) INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY  
10 INFORMATION, INCLUDING BROWSING HISTORY, SEARCH HISTORY, AND  
11 INFORMATION REGARDING AN INDIVIDUAL'S INTERACTION WITH AN INTERNET  
12 WEBSITE, APPLICATION, OR ADVERTISEMENT; AND

13 (VIII) A FINANCIAL OR OTHER ACCOUNT NUMBER, A CREDIT CARD  
14 NUMBER, OR A DEBIT CARD NUMBER THAT, IN COMBINATION WITH ANY REQUIRED  
15 SECURITY CODE, ACCESS CODE, OR PASSWORD, WOULD PERMIT ACCESS TO AN  
16 INDIVIDUAL'S ACCOUNT.

17 (2) "PERSONALLY IDENTIFIABLE INFORMATION" DOES NOT INCLUDE  
18 DATA RENDERED ANONYMOUS THROUGH THE USE OF TECHNIQUES, INCLUDING  
19 OBFUSCATION, DELEGATION AND REDACTION, AND ENCRYPTION, SO THAT THE  
20 INDIVIDUAL IS NO LONGER IDENTIFIABLE.

21 (G) "PROCESSING" MEANS ANY OPERATION OR SET OF OPERATIONS THAT  
22 IS PERFORMED ON PERSONALLY IDENTIFIABLE INFORMATION OR ON A SET OF  
23 PERSONALLY IDENTIFIABLE INFORMATION, WHETHER OR NOT BY AUTOMATED  
24 MEANS, INCLUDING COLLECTION, RECORDING, ORGANIZATION, STRUCTURING,  
25 STORAGE, ADAPTION OR ALTERATION, RETRIEVAL, CONSULTATION, USE,  
26 DISCLOSURE BY TRANSMISSION, DISSEMINATION, OR OTHERWISE MAKING  
27 AVAILABLE, ALIGNMENT OR COMBINATION, RESTRICTION, ERASURE, OR  
28 DESTRUCTION.

29 (H) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS  
30 SECURITY PROTECTIONS THAT ALIGN WITH THE CURRENT STANDARD OF CARE  
31 WITHIN SIMILAR COMMERCIAL ENVIRONMENTS AND WITH APPLICABLE STATE AND  
32 FEDERAL LAWS.

33 (I) "RECORDS" MEANS INFORMATION THAT IS INSCRIBED ON A TANGIBLE  
34 MEDIUM OR THAT IS STORED IN AN ELECTRONIC OR OTHER MEDIUM AND IS

1 RETRIEVABLE IN PERCEIVABLE FORM.

2 (J) "SYSTEM" MEANS AN ELECTRONIC OR OTHER PHYSICAL MEDIUM  
3 MAINTAINED OR ADMINISTERED BY THE UNIVERSITY SYSTEM OF MARYLAND AND  
4 USED ON A PROCEDURAL BASIS TO STORE INFORMATION IN THE ORDINARY COURSE  
5 OF THE BUSINESS OF THE UNIVERSITY.

6 (K) "UNIVERSITY" MEANS THE UNIVERSITY SYSTEM OF MARYLAND.

7 10-13A-02.

8 (A) THIS SUBTITLE DOES NOT APPLY TO PERSONALLY IDENTIFIABLE  
9 INFORMATION THAT:

10 (1) IS PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE  
11 AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL  
12 GOVERNMENT RECORDS;

13 (2) AN INDIVIDUAL HAS CONSENTED TO HAVE PUBLICLY  
14 DISSEMINATED OR LISTED;

15 (3) EXCEPT FOR A MEDICAL RECORD THAT A PERSON IS PROHIBITED  
16 FROM REDISCLOSING UNDER § 4-302(D) OF THE HEALTH - GENERAL ARTICLE, IS  
17 DISCLOSED IN ACCORDANCE WITH THE FEDERAL HEALTH INSURANCE  
18 PORTABILITY AND ACCOUNTABILITY ACT;

19 (4) IS DISCLOSED IN ACCORDANCE WITH THE FEDERAL FAMILY  
20 EDUCATIONAL RIGHTS AND PRIVACY ACT; OR

21 (5) IS CLINICAL INFORMATION RELATED TO SPONSORED RESEARCH.

22 (B) COMPLIANCE WITH THIS SUBTITLE DOES NOT AUTHORIZE THE  
23 UNIVERSITY SYSTEM OF MARYLAND TO FAIL TO COMPLY WITH ANY OTHER  
24 REQUIREMENTS OF STATE OR FEDERAL LAW RELATING TO THE PROTECTION AND  
25 PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION.

26 10-13A-03.

27 (A) THE UNIVERSITY SYSTEM OF MARYLAND SHALL REVIEW AND  
28 DESIGNATE SYSTEMS WITHIN THE UNIVERSITY AS SYSTEMS OF RECORD BASED ON  
29 THE FOLLOWING CRITERIA:

30 (1) THE RISK POSED TO INDIVIDUALS BY THE PERSONALLY

1 IDENTIFIABLE INFORMATION PROCESSED AND STORED ON THE SYSTEMS;

2 (2) THE RELATIONSHIP OF THE SYSTEMS TO THE OVERALL FUNCTION  
3 OF THE UNIVERSITY; AND

4 (3) THE TECHNICAL AND FINANCIAL FEASIBILITY OF IMPLEMENTING  
5 PRIVACY CONTROLS AND SERVICES WITHIN THE SYSTEM.

6 (B) THE UNIVERSITY SHALL DEVELOP AND ADOPT A PRIVACY GOVERNANCE  
7 PROGRAM TO GOVERN EACH SYSTEM OF RECORD THAT:

8 (1) IDENTIFIES AND DOCUMENTS THE PURPOSE OF THE UNIVERSITY  
9 IN PROCESSING PERSONALLY IDENTIFIABLE INFORMATION;

10 (2) PROHIBITS THE DISCLOSURE OF PERSONALLY IDENTIFIABLE  
11 INFORMATION TO THIRD PARTIES, OTHER THAN THOSE THIRD PARTIES  
12 PROCESSING PERSONALLY IDENTIFIABLE INFORMATION ON BEHALF OF THE  
13 UNIVERSITY, UNLESS:

14 (I) THE INDIVIDUAL CONSENTS TO DISCLOSURE OF THE  
15 INFORMATION; OR

16 (II) THE UNIVERSITY DETERMINES THAT DISCLOSURE OF THE  
17 INFORMATION IS IN THE BEST INTEREST OF THE UNIVERSITY;

18 (3) REQUIRES ALL AGREEMENTS ENTERED INTO WITH THIRD  
19 PARTIES ON OR AFTER OCTOBER 1, 2022, TO INCLUDE LANGUAGE REQUIRING THE  
20 THIRD PARTY TO SUPPORT THE UNIVERSITY'S PRIVACY GOVERNANCE PROGRAM;

21 (4) ENSURES THAT A THIRD PARTY PROCESSING PERSONALLY  
22 IDENTIFIABLE INFORMATION ON BEHALF OF THE UNIVERSITY ACTS IN  
23 ACCORDANCE WITH THE UNIVERSITY'S PRIVACY GOVERNANCE PROGRAM;

24 (5) TAKES REASONABLE STEPS TO ENSURE THAT PERSONALLY  
25 IDENTIFIABLE INFORMATION PROCESSED BY THE UNIVERSITY IS ACCURATE,  
26 RELEVANT, TIMELY, AND COMPLETE;

27 (6) TAKES REASONABLE STEPS TO ENSURE THAT REQUESTS TO  
28 ACCESS, MODIFY, OR DELETE INFORMATION AND REQUESTS TO OPT OUT OF THE  
29 SHARING OF INFORMATION WITH THIRD PARTIES ARE MADE BY THE SUBJECT OF  
30 THE PERSONALLY IDENTIFIABLE INFORMATION OR THE SUBJECT'S AGENT;

31 (7) TAKES REASONABLE STEPS TO LIMIT THE PERSONALLY

1 IDENTIFIABLE INFORMATION COLLECTED TO THAT INFORMATION NECESSARY TO  
2 ADDRESS THE PURPOSE OF THE COLLECTION;

3 (8) IMPLEMENTS A PROCESS TO PROVIDE INDIVIDUALS WITH ACCESS  
4 TO THE PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL  
5 HELD AND PROCESSED BY THE UNIVERSITY;

6 (9) PROVIDES INDIVIDUALS WITH A PROCESS TO REQUEST A  
7 CORRECTION TO PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE  
8 INDIVIDUAL;

9 (10) IN THE CASE OF A DISAGREEMENT BETWEEN THE UNIVERSITY  
10 AND AN INDIVIDUAL OVER THE ACCURACY OF PERSONALLY IDENTIFIABLE  
11 INFORMATION RELATING TO THE INDIVIDUAL, PROVIDES A MEANS FOR THE  
12 INDIVIDUAL TO DOCUMENT THE DISAGREEMENT AND PRODUCE THE  
13 DOCUMENTATION OF THE DISAGREEMENT WHENEVER THE DISPUTED  
14 INFORMATION IS PRODUCED;

15 (11) PROVIDES A PROCESS FOR INDIVIDUALS TO REQUEST THE  
16 DELETION OF PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE  
17 INDIVIDUAL THAT THE UNIVERSITY DOES NOT HAVE A LEGITIMATE BASIS TO  
18 PROCESS;

19 (12) PROVIDES A PROCESS FOR INDIVIDUALS TO OPT OUT OF SHARING  
20 PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL WITH  
21 THIRD PARTIES, IF THE UNIVERSITY WOULD NOT HAVE A LEGITIMATE BASIS TO  
22 PROCESS THE INFORMATION; AND

23 (13) PROVIDES A PROCESS FOR THE UNIVERSITY TO CONSIDER  
24 REQUESTS MADE UNDER THIS SUBSECTION THAT ALLOWS THE UNIVERSITY TO DENY  
25 A REQUEST IF THE UNIVERSITY REASONABLY CONCLUDES IT HAS A LEGITIMATE  
26 BASIS FOR PROCESSING THE PERSONALLY IDENTIFIABLE INFORMATION OR IF THE  
27 REQUEST IS NOT TECHNICALLY OR FINANCIALLY FEASIBLE.

28 (C) THE UNIVERSITY SHALL DEVELOP AND ADOPT AN INFORMATION  
29 SECURITY AND RISK MANAGEMENT PROGRAM FOR THE PROTECTION OF  
30 PERSONALLY IDENTIFIABLE INFORMATION THAT SHALL:

31 (1) IMPLEMENT REASONABLE SECURITY PROCEDURES AND  
32 PRACTICES, COMPATIBLE WITH APPLICABLE FEDERAL AND STATE STANDARDS AND  
33 GUIDELINES, TO ENSURE THAT THE RISK TO THE CONFIDENTIALITY, INTEGRITY,  
34 AND AVAILABILITY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IS PROPERLY  
35 MANAGED;

1           **(2) BE PERIODICALLY ASSESSED BY A THIRD PARTY ASSESSOR WITH**  
2 **EXPERTISE IN INFORMATION SECURITY;**

3           **(3) BE APPROVED BY AN APPROPRIATE SENIOR OFFICIAL OF THE**  
4 **UNIVERSITY WITH AUTHORITY TO ACCEPT RISK FOR THE UNIVERSITY;**

5           **(4) REQUIRE THAT CONTRACTS WITH THIRD PARTIES INCLUDE**  
6 **PROVISIONS TO ENSURE THAT THIRD PARTIES THAT PROCESS PERSONALLY**  
7 **IDENTIFIABLE INFORMATION ON BEHALF OF THE UNIVERSITY MAINTAIN**  
8 **APPROPRIATE SECURITY CONTROLS COMMENSURATE WITH THE RISK POSED TO THE**  
9 **INDIVIDUALS BY THE PERSONALLY IDENTIFIABLE INFORMATION; AND**

10           **(5) ENSURE THAT ANY BREACHES BY THE UNIVERSITY OR A THIRD**  
11 **PARTY ACTING ON BEHALF OF THE UNIVERSITY ARE PROPERLY DOCUMENTED,**  
12 **INVESTIGATED, AND REPORTED TO APPROPRIATE AUTHORITIES WITHIN THE**  
13 **UNIVERSITY.**

14           **(D) (1) THE UNIVERSITY SHALL PUBLISH A PRIVACY NOTICE ON THE**  
15 **UNIVERSITY'S WEBSITE THAT IS:**

16                   **(I) WRITTEN IN PLAIN LANGUAGE; AND**

17                   **(II) DIRECTLY ACCESSIBLE FROM THE UNIVERSITY'S**  
18 **HOMEPAGE AND ANY OF THE UNIVERSITY'S WEBPAGES THAT ARE USED TO COLLECT**  
19 **PERSONALLY IDENTIFIABLE INFORMATION.**

20           **(2) THE NOTICE PUBLISHED UNDER PARAGRAPH (1) OF THIS**  
21 **SUBSECTION SHALL INCLUDE:**

22                   **(I) THE TYPES OF PERSONALLY IDENTIFIABLE INFORMATION**  
23 **COLLECTED BY THE UNIVERSITY;**

24                   **(II) THE PURPOSE OF THE COLLECTION, USE, AND SHARING OF**  
25 **PERSONALLY IDENTIFIABLE INFORMATION BY THE UNIVERSITY; AND**

26                   **(III) THE PROCESSES BY WHICH AN INDIVIDUAL MAY REQUEST:**

27                           **1. TO HAVE PERSONALLY IDENTIFIABLE INFORMATION**  
28 **RELATED TO THE INDIVIDUAL CORRECTED;**

29                           **2. TO HAVE PERSONALLY IDENTIFIABLE INFORMATION**  
30 **RELATED TO THE INDIVIDUAL DELETED;**



1                   **3. INFORMATION ON THE SHARING OF PERSONALLY**  
2 **IDENTIFIABLE INFORMATION BY THE UNIVERSITY WITH THIRD PARTIES,**  
3 **INCLUDING A LISTING OF THE THIRD PARTIES, A LISTING OF THE INFORMATION**  
4 **SHARED, AND THE PURPOSE OF SHARING THE INFORMATION; AND**

5                   **4. TO OPT OUT OF THE SHARING OF PERSONALLY**  
6 **IDENTIFIABLE INFORMATION WITH A THIRD PARTY.**

7                   **(3) THE UNIVERSITY SHALL ENSURE ACCESS CONTROLS ARE IN**  
8 **PLACE TO ADDRESS ANY SECURITY RISKS POSED BY PROVIDING THE NOTICE**  
9 **REQUIRED UNDER THIS SUBSECTION.**

10                   **(E) WHEN THE UNIVERSITY IS DESTROYING RECORDS OF AN INDIVIDUAL**  
11 **THAT CONTAIN PERSONALLY IDENTIFIABLE INFORMATION OF THE INDIVIDUAL, THE**  
12 **UNIVERSITY SHALL TAKE REASONABLE STEPS TO PROTECT AGAINST**  
13 **UNAUTHORIZED ACCESS TO OR USE OF THE PERSONALLY IDENTIFIABLE**  
14 **INFORMATION, TAKING INTO ACCOUNT:**

15                   **(1) THE SENSITIVITY OF THE RECORDS;**

16                   **(2) THE NATURE OF THE UNIVERSITY AND ITS OPERATIONS;**

17                   **(3) THE COSTS AND BENEFITS OF DIFFERENT DESTRUCTION**  
18 **METHODS; AND**

19                   **(4) AVAILABLE TECHNOLOGY.**

20 **10-13A-04.**

21                   **(A) IF THE UNIVERSITY COLLECTS PERSONALLY IDENTIFIABLE**  
22 **INFORMATION OF AN INDIVIDUAL AND DISCOVERS OR IS NOTIFIED OF A BREACH OF**  
23 **THE SECURITY OF A SYSTEM, THE UNIVERSITY SHALL CONDUCT IN GOOD FAITH A**  
24 **REASONABLE AND PROMPT INVESTIGATION TO DETERMINE WHETHER THE**  
25 **UNAUTHORIZED ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION OF**  
26 **THE INDIVIDUAL HAS OCCURRED.**

27                   **(B) (1) IF, AFTER THE INVESTIGATION IS CONCLUDED, THE UNIVERSITY**  
28 **DETERMINES THAT A BREACH OF THE SECURITY OF THE SYSTEM HAS OCCURRED,**  
29 **THE UNIVERSITY OR A THIRD PARTY, IF AUTHORIZED UNDER A WRITTEN CONTRACT**  
30 **OR AGREEMENT WITH THE UNIVERSITY, SHALL:**

31                   **(I) NOTIFY THE INDIVIDUAL OF THE BREACH; AND**

1                   **(II) NOTIFY THE UNIVERSITY’S CHIEF INFORMATION OFFICER**  
2 **OF THE BREACH.**

3                   **(2) A NOTIFICATION REQUIRED UNDER PARAGRAPH (1) OF THIS**  
4 **SUBSECTION SHALL INCLUDE, TO THE EXTENT POSSIBLE, A DESCRIPTION OF THE**  
5 **CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION THAT WERE, OR ARE**  
6 **REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED BY AN UNAUTHORIZED PERSON,**  
7 **INCLUDING WHICH OF THE ELEMENTS OF PERSONALLY IDENTIFIABLE**  
8 **INFORMATION WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED.**

9                   **(3) IF THE UNIVERSITY DETERMINES THAT A BREACH OF THE**  
10 **SECURITY OF THE SYSTEM HAS OCCURRED INVOLVING THE PERSONALLY**  
11 **IDENTIFIABLE INFORMATION OF 1,000 OR MORE INDIVIDUALS, THE UNIVERSITY**  
12 **SHALL POST A NOTICE ON THE SAME WEBPAGE AS THE UNIVERSITY’S PRIVACY**  
13 **NOTICE WEBSITE:**

14                   **(I) DESCRIBING THE BREACH; AND**

15                   **(II) THAT REMAINS PUBLICLY AVAILABLE ON THE WEBSITE FOR**  
16 **AT LEAST 5 YEARS FROM THE DATE ON WHICH NOTICE WAS SENT TO INDIVIDUALS**  
17 **AFFECTED BY THE BREACH.**

18                   **SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect**  
19 **October 1, 2022.**