

Personal Information Security Breach Notification Protocol

The University of North Carolina at Pembroke

I. Introduction

The North Carolina Identity Theft Protection Act, S.L. 2005-414, requires State agencies to notify persons whose personal information held by an agency has or may have been compromised by a breach of the agency's security. This Protocol sets forth the circumstances and procedures under which required notification will be made.

II. Definition

A. **“Personal Information”** is defined by the Act and this policy to mean a person's first name or first initial and last name in combination with any of the following items for purposes of this policy:

1. Social security or employer taxpayer identification number;
2. Drivers license, State identification card, or passport numbers;
3. Checking account numbers;
4. Savings account numbers;
5. Credit card numbers;
6. Debit card numbers;
7. Personal Identification Number (PIN code);
8. Digital signatures;
9. Any other numbers or information that can be used to access a person's financial resources;
10. Biometric data;
11. Fingerprints; or
12. Passwords.

Under the Act and this policy, the definition of “personal information” specifically **excludes** “electronic identification numbers (*i.e.*, *Banner ID numbers*), electronic mail names or addresses, Internet account numbers, or Internet identification names, parent's legal surname prior to marriage, or drivers license numbers appearing on law enforcement records” when possessed by a university. Disclosure of these specifically excluded items from education records may be prohibited by the Family Education Rights and Privacy Act, 20

U.S.C. § 1232g (34 CFR Part 99, et seq.) or other University policy, but disclosures of these specifically listed exclusions are not covered by this policy. Therefore, improperly disclosing a student’s Banner ID number may be a violation of FERPA, but notification regarding that disclosure would not be required under this policy or the Act.

Personal information does not include publicly available directories containing information that an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, State, or local government records.

- B. **“Security Breach”** is defined by the Act to mean: an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach (except see Endnote 1, herein).

Good faith acquisition of personal information by an employee or agent of the University for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the University and is not subject to further unauthorized disclosure.

III. **Procedures in the Event of a Security Breach**

A. **Containment, Classification, and Report of a Breach.**

1. **Containment:** The first priority after a security breach is discovered is to contain the breach and notify supervisory personnel as quickly as possible. For any category of breach, the data must be secured, and the reasonable integrity, security, and confidentiality of the data or data system must be restored.
2. **Classification:** The next step is to determine the exact nature of the breach in terms of its extent and seriousness. For these purposes, breaches may fall into one of three categories:
 - **Category I:** Unauthorized access to and use of the personal information has been confirmed.

- **Category II:** Unauthorized access to the personal information has been confirmed and unauthorized use is reasonably likely to occur (including instances of unauthorized access to and acquisition of encrypted records or data containing personal information along with the taking of the confidential process or key).
 - **Category III:** Personal information is easily accessible¹ to unauthorized persons due to flaws in the security system, loss of storage media, or other failure to account for the whereabouts or status of personal information, but there is no confirmation that unauthorized access to or use of personal information has yet occurred.
3. **Internal Reporting of a Breach:** As soon as a breach has been identified, the employee who discovered it must take immediate steps to report the breach to his or her supervisor. The supervisor must take immediate action to determine the extent and category of the breach and to take such further action as is necessary to contain the breach or recover the missing data. Assistance from University Computing and Information Services, University Police, or other office with relevant expertise should be requested as soon as possible. For example, if the potential or actual breach involves electronic equipment, the UNCP Chief Information Officer must be immediately notified. If the potential or actual breach involves loss or theft of University-owned equipment or other criminal activity, notify the University Police.² In all cases of a breach, University Counsel's Office must be notified as soon as practicable.

The supervisor must document the breach, noting the category involved, the scope of the breach, steps taken to contain the breach, and the names or categories of persons whose personal information was, or may have been, acquired by an unauthorized person. A copy of that documentation must be sent to University Counsel

B. Notification to Victims

1. **Time for Providing Notification.** The University shall notify affected individuals without unreasonable delay upon discovery of a Category I or II breach.³ However, notification shall be delayed if law enforcement

informs the University that disclosure of the breach would impede a criminal investigation or jeopardize national or homeland security. A request for delayed notification must be made in writing or documented contemporaneously by the University in writing, including the name of the law enforcement officer making the request and the officer's agency engaged in the investigation. The required notification shall be provided without unreasonable delay after the law enforcement agency communicates to the University its determination that notification will no longer impede the investigation or jeopardize national or homeland security.

2. **Responsibility for Providing Notification.** The responsibility for providing notification shall lie with the Head of the Division that has primary authority for the data. If the breach involves data from more than one Division or if primary authority for the data cannot be determined, the responsibility shall lie with the Chancellor. The Division Head or the Chancellor may delegate this responsibility, but should satisfy himself or herself that the proper notification has, in fact, occurred. The University Counsel will review the proposed notification before it is sent and will assist in drafting as required. A copy of the notification will also be provided to the Director of University Relations prior to the time it is posted or sent to affected individuals.
3. **Contents of the Notification.** Notification shall be clear and conspicuous and include a description of the following:
 - a. The incident in general terms.
 - b. The type of personal information that was subject to the unauthorized access and acquisition.
 - c. The actions taken by the University to protect the personal information from further unauthorized access. However, the description of those actions may be general so as not to further increase the risk or severity of the breach.
 - d. A telephone number that the person may call for further information and assistance.
 - e. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

4. **Method of Notification.** Notification to affected persons must be provided by one of the following methods⁴ unless substitute notification is permitted:
 - . Written notification, or
 - a. Electronic notification, for those persons for whom the University has a valid e-mail address and who have agreed to receive communications electronically, or
 - b. Telephonic notification provided that contact is made directly with the affected persons.

5. **Substitute Notification.** Substitute notification may be given if:
 - . The cost of providing the notification exceeds \$250,000;
 - a. The cost of providing the notification exceeds \$250,000;
 - b. The University does not have the necessary contact information to notify an individual in any of the aforementioned manners; or
 - c. The University is not able to identify particular affected individuals.

Substitute notification shall include all of the following:

- d. E-mail notification when the University has an electronic e-mail address for subject persons;
 - e. Conspicuous posting of the notification on the University's Web page; and
 - f. Notification to major statewide media.
6. **Additional Notification Requirements.** If a security breach involves notification to more than 1,000 persons, the University Counsel shall notify, without unreasonable delay, the Consumer Protection Division of the North Carolina Attorney General's Office, as well as all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of any notification. In addition, the University Counsel shall submit to the Consumer Protection Division a completed "North Carolina Security Breach Reporting Form" which includes the number of North Carolina residents affected and the total number of persons affected.

IV. Effective Date

This is effective immediately.

This policy is copied with permission from The University of North Carolina at Greensboro, with a few modifications.

Last modified: July 25, 2007

¹ The term “easily accessible” means accessible to a person who does not possess sophisticated computing or decoding skills.

² In this instance, the State Bureau of Investigation must also be notified in accordance with N.C.Gen.Stat. §114-15.1.

³ Although notification in case of a Category III breach is not required by the Identity Theft Protection Act, the Chancellor, in his or her sole discretion, may direct that notification be given, if, under the facts and circumstances surrounding the breach, the Chancellor believes it to be in the best interest of the University and of individuals whose personal information may have been put at risk.

⁴ Although the Identity Theft Protection Act only requires that one of the options listed in this section be selected, the University has discretion to give notice by more than one method.