Personal Information Security Breach Notification Policy

Approved by Cabinet on September 4, 2013

Purpose:

The North Carolina Identity Theft Protection Act requires organizations to notify persons whose personal information held by the organization has been compromised by an information security breach.

The purpose of this policy is to define the circumstances and procedures under which required notifications will be made.

Scope:

This policy applies to all Catawba College students, faculty, and staff.

Definitions:

Personal Information is defined by the North Carolina Identity Theft Protection Act as a person's first name or first initial and last name in combination with any of the following items:

- Social Security or employer taxpayer identification number
- Driver's license, state identification card, or passport numbers
- Checking account numbers
- Savings account numbers
- Credit or debit card numbers
- Personal Identification Number (PIN code)
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints

- Even if listed above, however, "personal information" does not include publicly available directories containing information 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.

Information Security Breach is defined as 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, also constitutes an information security breach.

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

Policy:

- Any information security breach should be reported to the Chief Information Officer (CIO) and the IT Security Administrator immediately upon discovery.
- In the case of an information security breach that results in disclosure of personal information, Catawba will notify the affected individuals without unreasonable delay.
- Notification will be delayed if a law enforcement agency determines that notification will impede a criminal investigation.

    - In this case, notification will be provided without unreasonable delay after the law enforcement agency determines that it will not compromise the investigation.
- A copy of the notification will also be provided to the Chief Communications Officer prior to the time it is posted or sent to affected individuals.
- The notification will be clear and conspicuous and include all of the following:
    - A description of the incident in general terms
    - A description of the type of personal information that was subject to the unauthorized access and acquisition
    - A description of the actions taken by the College 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.
    - A telephone number that the person may call for further information and assistance
    - Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports
    - The toll-free numbers and addresses for the major consumer reporting agencies
    - The toll-free numbers, addresses, and web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.
- Notification to those affected will be provided by one of the following methods unless substitute notification is permitted:
    - Written notification, or
    - Electronic notification, for those persons whom the College has a valid e-mail address and who have agreed to receive communications electronically, or

  - Telephonic notification provided that the contact is made directly with the affected persons.
- Substitute notification may be given if:
  - The cost of providing the notification exceeds $250,000; or
  - The College does not have the necessary contact information to notify an individual in any of the aforementioned manners; or
  - The College is not able to identify particular affected individuals.
- If given, substitute notification will include all of the following:
  - E-mail notification when the College has an electronic e-mail address for subject persons;
  - Conspicuous posting of the notification on the College's web page; and
  - Notification to major statewide media.
- Whenever notice of an information security breach as defined by this Policy is given to at least one person, the College, without unreasonable delay, will notify the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.
- Whenever notice of an information security breach as defined by this Policy is given to more than 1,000 persons, the College will notify, without unreasonable delay, all three major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.