Policy Information

Series 4000 - Non-Instructional/Business Operation

Information Security Breach & Notification
Policy # 4580, 5.8

POLICY

2006 4580

Non-Instructional/Business Operations

SUBJECT: *INFORMATION SECURITY BREACH AND NOTIFICATION

The BOCES values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

a. "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

    1. Social security number;

    2. Driver's license number or non-driver identification card number; or

    3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

    "Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

    **"Personal information" shall mean any information concerning a person which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b. "Breach of the security of the system," shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the BOCES. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Examples of Determining Factors

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the BOCES may consider the following factors, among others:

a. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

b. Indications that the information has been downloaded or copied; or

c. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Notification Requirements

a. For any computerized data owned or licensed by the BOCES that includes private information, the BOCES shall disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The BOCES shall consult with the State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.

b. For any computerized data maintained by the BOCES that includes private information which the BOCES does not own, the BOCES shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.

Methods of Notification

The required notice shall be directly provided to the affected persons by one of the following methods:

a. Written notice;

b. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

c. Telephone notification, provided that a log of each such notification is kept by the BOCES when notifying affected persons by phone; or

d. Substitute notice, if the BOCES demonstrates to the State Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the BOCES does not have sufficient contact information. Substitute notice shall consist of all of the following:

    1. E-mail notice when the BOCES has an e-mail address for the subject persons;

    2. Conspicuous posting of the notice on the BOCES' website page, if the BOCES maintains one; and

    3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to

have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

In the event that any New York State residents are to be notified, the BOCES shall notify the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents.

In the event that more than 5,000 New York State residents are to be notified at one time, the BOCES shall also notify consumer reporting agencies, as defined pursuant to State Technology Law Section 208, as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents. A list of consumer reporting agencies shall be compiled by the State Attorney General and furnished upon request to school districts required to make a notification in accordance with Section 208(2) of the State Technology Law, regarding notification of breach of security of the system for any computerized data owned or licensed by the BOCES that includes private information.

State Technology Laws Section 202 and 208

Board Approved
04/19/06

Adoption Date: 4/19/2006
4000 - Non-Instructional/Business Operation