NYSSBA Sample Policy 8635

(X) Required
(X) Local
(X) Notice

INFORMATION SECURITY BREACH AND NOTIFICATION

NOTE: With heightened attention on the need for districts to protect personally identifiable data, NYSSBA reviewed this policy and offers some enhancements. In addition, we have added cross-references to related policies. Districts are reminded that personally identifying information is still stored as hard copy and needs to be protected to the same degree as digitally stored information.

There is some ambiguity about whether school districts are legally required to have a policy on this topic; NYSSBA views it as required. Whether or not it is required, in view of the current attention to this issue, Boards are urged to have a policy in place.

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. To this end, the Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure. For purposes of this policy, "private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

Additionally, pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes social security number, home address or telephone number, personal electronic email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, the district will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed, be printed on any ID badge, card or time card, be placed in files with unrestricted access, or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district shall be promptly reported to the Superintendent and the Board of Education.

Cross-ref: 1120, District Records
5500, Student Records
8630, Computer Resources and Data Management

NYSSBA Sample Policy 8635

Ref: State Technology Law §§201-208
Labor Law §203-d

Adoption date:

NYSSBA Sample Regulation 8635-R

INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION

NOTE: In the case of a breach of information that meets the definition of the Labor Law's personal identifying information, but not the Technology Law's definition, NYSSBA recommends consulting with the district's school attorney as to whether notification is required or advisable. Bear in mind the intent of both laws is to limit identity theft and protect privacy.

Definitions

"Private information" shall mean personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) 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:

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

NOTE: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.

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

To successfully implement this policy, the district shall inventory its hard copy, computer programs and electronic files to determine the types of personal, private information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district shall consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of hard copies, lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded, removed or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts, opened or instances of identity theft reported; and/or
4. any other factors which the district shall deem appropriate and relevant to such determination.

Security Breaches – Procedures and Methods for Notification

Once it has been determined that a security breach has occurred, the following steps shall be taken:

1. If the breach involved hard copy or computerized data *owned or licensed* by the district, the district shall notify those New York State residents 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 to restore the reasonable integrity of the system.

   The district shall consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures.
2. If the breach involved hard copy or computer data *maintained* by the district, the district shall notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been acquired by a person without valid authorization.

NOTE: 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.

The required notice shall include (a) district contact information, (b) a description of the categories information that were or are reasonably believed to have been acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) what the district is doing about it . This notice shall be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of each such electronic notification. In no case, however, shall the district require a person

to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.

3. Telephone notification, provided that the district keeps a log of each such telephone notification.

However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the district has such address for the affected individual;
2. Conspicuous posting on the district's website, if they maintain one; and
3. Notification to major media

Notification of State and Other Agencies

NOTE: Following a reorganization of state agencies, the State Technology Law §208(7) was revised with respect to the agencies which must receive notification.

Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the Department of State Division of Consumer Protection, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the district shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

Adoption date: