Information Security and Incident Response

Data Breaches Requiring Notifications to Third Parties

Definitions

Some terminology with a wide general application is used more narrowly in this policy to denote specific District cybersecurity practices and legal obligations. As a result, the definitions below apply only to this regulation.

Breach of the security of the system. The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the District for the purposes of the District is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the District and is not subject to further unauthorized disclosure.

Determination. A verification or reasonable certainty that a breach of the security system has occurred.

Discovery. The knowledge of or reasonable suspicion that a breach of the security of the system has occurred.

Health insurance information: An individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.

"Notice." An alert to affected individuals that their personal information has been or may have been accessed and acquired by an unauthorized person. "Notice" may refer to any of the following methods of notification:

1. Written notice to the last known home address for the individual.
2. Telephonic notice, if the individual can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the individual to provide personal information and the individual is provided with a telephone number to call or Internet website to visit for further information or assistance.
3. E-mail notice, if a prior business relationship exists and the District has a valid e-mail address for the individual.

4. Electronic notice, if the notice directs the person whose personal information has been materially compromised by a breach of the security of the system to promptly change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the person's online account to the extent the entity has sufficient contact information for the person..
    i) Substitute notice, if the District demonstrates one of the following:
        (1) The cost of providing notice would exceed $100,000.
        (2) The affected class of subject persons to be notified exceeds 175,000.
        (3) The entity does not have sufficient contact information.
    ii) Substitute notice shall consist of all of the following:
        (1) E-mail notice when the District has an e-mail address for the subject persons.
        (2) Conspicuous posting of the notice on the District's Internet website if the entity maintains one.
        (3) Notification to major Statewide media.

Personal information:

1. An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
    i) Social Security number.
    ii) Driver's license number or a State identification card number issued in lieu of a driver's license.
    iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
    iv) Medical information.
    v) Health insurance information.
    vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.
2. The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media.

Records: Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not

include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

Redact: The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data.

Notice

A. Timing

Within three (3) days of determination of a breach, the Superintendent or their designee shall provide notification of the breach to the Chester County district attorney.

Within seven (7) days of determination of a breach, the District shall notify any Pennsylvania resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Pennsylvania residency shall be determined by the principal mailing address of an individual as it appears in the District's databases.

B. Delay

The notification required by this act may be delayed if a law enforcement agency determines and advises the District in writing, specifically referencing 73 P.S.§ 2304, that the notification will impede a criminal or civil investigation. The District shall then make any required notification only after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

C. Electronic Notice

In the event that the breach involves personal information for a user name or e-mail address in combination with a password or security question or answer that would permit access to an online account, the District may notify affected individuals by email. The content of this email must disclose what categories of personal information have been materially compromised by the breach (i.e. email and password or security question), and shall direct the recipient to change their password and security question or to take other steps appropriate to protect both the breached account and any other online accounts that use the same security information.

D. Notification of consumer reporting agencies

In the event the District must provide notification to more than 1,000 persons at one time, the District shall also notify, without unreasonable delay, all consumer

reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

E. Vendor notification

A vendor that maintains, stores or manages computerized data on behalf of the District shall provide notice of any breach of the security of a system following discovery by the vendor to the District on whose behalf the vendor maintains, stores or manages the data. The District shall be responsible for making any determinations and discharging any remaining duties as required by this policy.

Other Security Incidents

Examples of other security incidents contemplated in the accompanying Board Policy include, but are not limited to:

- Unauthorized access to applications, systems, data storage, network devices, firewalls, or any computer resource;
- Intentionally targeted, but unsuccessful unauthorized access;
- Accidental or malicious disclosure/loss of restricted or confidential information;
- Infection by malware;
- Denial-of-service attack;
- Theft or physical loss of computer equipment, tablets, smartphones, mobile devices, or similar systems known to store restricted or confidential information;
- Violating any Board Policy or procedure related to information security;
- Virus or worm using open file shares to infect computer or similar systems;
- An attacker runs an exploit tool to gain access to a District server's password file;
- Any event that threatens the confidentiality, integrity, or availability of District systems, applications, data, or networks.

Overview of Critical Roles

- Incident Executive Oversight: This role is filled by the Director of Educational Program or designee.

- Incident Manager: This role is filled by the Director of Educational Program or designee.

- System/Applications Administrator: This role is filled by the technical staff responsible for deploying and maintaining the affected systems and applications.

- System Owner: This role is filled by the staff member or management member who has responsibility for the business function performed by affected system/application.

- Network Administrator: This role is filled by the technical staff responsible for network infrastructure.

Guidelines

Anyone with knowledge or a reasonable suspicion of an incident which violates the confidentiality, integrity, or availability of digital information, or intrusion attempts, security breaches, theft or loss of hardware and other security related incidents perpetrated against the District must make an immediate report to the Director of Educational Program.

Any security incident that potentially endangers physical safety, involves restricted or confidential information, or disables critical services is deemed a Critical Information Security Incident (CISI).

The incident manager, in collaboration with other appropriate staff, shall determine if a reported incident is or is not a CISI.

If the incident is not considered a CISI, the incident shall be referred to a systems or network administrator, who shall ensure that the incident is handled in accordance with established procedures.

If the incident manager, in collaboration with other appropriate staff, determines that the incident is a CISI, an Incident Response Team (IRT) is formed. The purpose of the IRT is to determine a course of action to appropriately address the incident.

The Director of Educational Program shall designate the membership of the IRT. Normally, membership will include appropriate individuals from the Technology Department with primary responsibility for the compromised data.

It is the responsibility of the IRT to assess the actual or potential damage to the District caused by the CISI and execute a plan to mitigate that damage.

IRT members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation and approval from the Incident Executive Oversight.

The IRT will utilize established procedures as a guide when responding to any CISI.

The IRT shall prepare a report for every CISI describing the incident in detail, the circumstances that led to the incident, and a plan to eliminate the risk of a future occurrence.

Violation of this Administrative Regulation or the accompanying Board Policy may result in suspension or loss of network services, disciplinary action up to and including termination of employment, and/or legal action.