

**THORNBURY TOWNSHIP, DELAWARE COUNTY, PENNSYLVANIA**

**RESOLUTION NO. 9 OF 2023**

**A RESOLUTION OF THORNBURY TOWNSHIP, DELAWARE COUNTY, PENNSYLVANIA, ESTABLISHING A POLICY PROVIDING FOR SECURITY OF COMPUTERIZED DATA AND FOR THE NOTIFICATION OF RESIDENTS WHOSE PERSONAL INFORMATION DATA WAS OR MAY HAVE BEEN DISCLOSED DUE TO A BREACH OF THE SECURITY SYSTEM.**

**WHEREAS**, from time to time, electronic resident information and other important electronic data is provided to Thornbury Township, Delaware County (“Township”) in the ordinary course of the Township serving its residents and the community; and

**WHEREAS**, the Township and the Commonwealth of Pennsylvania, among others, recognize the importance of protecting such electronic data and information and maintaining same for the purpose(s) for which it was provided; and

**WHEREAS**, the Commonwealth of Pennsylvania has heretofore adopted the Breach of Personal Information Notification Act [Act of December, 22, 2005, P.L. 474, No 94], as amended by the Act of November 2, 2022, P.L. 2139, No. 151 (collectively the “Act”); and

**WHEREAS**, the purpose of the Act is to provide security for computerized data and for the notification of residents whose personal information data was or may have been disclosed due to a breach of the security of the system.

**WHEREAS**, the Township, in accordance with the Act, desires to adopt a policy providing for among other things, the notification of residents whose personal information data was or may have been disclosed due to a breach of the security of the system.

**NOW THEREFORE, BE IT RESOLVED**, that the Board of Supervisors of Delaware County, Pennsylvania, Pennsylvania, hereby approves and adopts the notification policy attached (the “Notification Policy”) hereto as and made a part hereof as **Exhibit “A”**, as the official policy of Thornbury Township, Delaware County, regarding the notification of residents in the event of a breach of personal information;

**AND BE IT FURTHER SOLVED**, that in accordance with such policy, the Township shall reexamine said policy from time to time by the Board of Supervisors, who may make updates, revisions and amendments, to such policy by official resolution.

**RESOLVED** and **APPROVED**, the \_\_\_\_\_ day of \_\_\_\_\_, 2023, to be effective on and after May 22, 2023, by the Board of Supervisors of Thornbury Township, Delaware County, Pennsylvania.

**BOARD OF SUPERVISORS  
TOWNSHIP OF THORNBURY,  
Delaware County**

\_\_\_\_\_  
James P. Kelly, Chairman

\_\_\_\_\_  
Sheri L. Perkins, Vice-Chair

\_\_\_\_\_  
Michael J. Mattson, Supervisor

ATTEST:

\_\_\_\_\_  
Geoffrey Carbutt, Township Secretary

(TOWNSHIP SEAL)

**EXHIBIT “A”**

**THORNBURY TOWNSHIP, DELAWARE COUNTY, PENNSYLVANIA**  
**BREACH OF PERSONAL INFORMATION NOTIFICATION POLICY**

**Section 1.     Short Name.**     This policy may be referred to as the “Thornbury Township Breach of Personal Information Notification Policy.”

**Section 2.     Purpose.**         The purpose of this policy is to provide for security of computerized data and for the notification of Township residents whose personal information data was or may have been disclosed to a breach of the Township’s security system or that of one of its vendors.

**Section 3.     Definitions.**     The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

“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 Township as part of a database of personal information regarding multiple individuals and that causes or the Township reasonably believes has caused or will cause loss or injury to any resident of the Township. Good faith acquisition of personal information by an employee or agent of the Township for the purposes of the Township 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 Township and is not subject to further unauthorized disclosure.

“Business.” A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

“Commonwealth”. The Commonwealth of Pennsylvania.

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

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

“Encryption.” The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

“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.

“Individual.” A natural person.

“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.

“Medical information.” Any individually identifiable information contained in the individual’s current or historical record of medical history or medical treatment or diagnosis created by a health care professional.

“Notice or Notification.” Any of the following methods:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the [customer] 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 [customer] individual to provide personal information and the [customer] 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 person or Township has a valid e-mail address for the individual.

(3.1) 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 Township has sufficient contact information for the person.

(4) (i) Substitute notice, if the Township demonstrates one of the following:

(A) The cost of providing notice would exceed \$100,000.

(B) The affected class of subject persons to be notified exceeds 175,000.

(C) The Township does not have sufficient contact information.

(ii) Substitute notice shall consist of all of the following:

(A) E-mail notice when the Township has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Township’s Internet website.

(C) 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 username 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.

“Township”. Thornbury Township, Delaware County, Pennsylvania.

“Township contractor.” A person, business, subcontractor or third party subcontractor that has a contract with the Township for goods or services that requires access to any personal information for the fulfillment of the contract.

**Section 3.** General rule. In cases where the Township maintains, stores or manages computerized data that includes personal information, the Township shall provide notice of any breach of the security of the system following determination of the breach of the security of the system to any resident of the Township whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in Section 7, below, or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the Township, is in the Commonwealth.

**Section 4.** Notification by Township. If the Township is the subject of a breach of the security of the system, the Township shall provide notice of the breach of the security of the system required under Section 3, above within seven (7) business days following determination of the breach of the security of the system. Notification shall be provided to the District Attorney of Delaware County within three (3) business days following determination of the breach of the security of the system.

**Section 5.** Electronic notification. In the case of a breach of the security of the system involving personal information for a username or e-mail address in combination with a password or security question and answer that would permit access to an online account, the Township, to the extent that it has sufficient contact information for the person, may comply with this Section by providing the breach of the security of the system notification in electronic or other form that directs the person whose personal information has been materially compromised by the 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 online account with the Township and other online accounts for which the person whose personal information has been materially compromised by the breach of the security of the system uses the same user name or e-mail address and password or security question or answer.

**Section 6.** Affected Individuals. In the case of a breach of the security of the system involving personal information of an individual's username or e-mail address in combination with a password or security question and answer that would permit access to an online account, a Township contractor may comply with this Section by timely providing a list of affected residents and their valid e-mail addresses, if known, to the Township. The Township shall be responsible for making the determinations and discharging any remaining duties under this policy.

**Section 7.** Delay in notification. The notification required by this policy may be delayed if a law enforcement agency determines and advises the Township in writing specifically referencing this Section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

**Section 8.** Large scale notification. When the Township provides notification under this policy to more than 1,000 persons at one time, the Township 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.

**Section 9.** Encryption Required.

(a) General Rule. A Township contractor that maintains, stores or manages computerized data on behalf of the Township that constitutes personal information shall utilize encryption, or other appropriate security measures, to reasonably protect the transmission of personal information over the Internet from being viewed or modified by an unauthorized third party.

(b) Transmission policy. A Township contractor that maintains, stores or manages computerized data on behalf of the Township that constitutes personal information shall develop and maintain a policy to govern the proper encryption or other appropriate security measures and transmission of data established by the Federal Government and the Commonwealth.

(c) Considerations. In developing the policy, a Township contractor shall reasonably consider similar existing Federal policies and other policies, best practices identified by other

states and relevant studies and other sources as appropriate in accordance with best practices as established by the Federal Government and the Commonwealth.

(d) Review and update. The policy shall be reviewed at least annually and updated as necessary.

**Section 10.** Data storage policy.

(a) Storage policy.—A Township contractor that maintains, stores or manages computerized data on behalf of the Township that constitutes personal information shall develop a policy to govern reasonably proper storage of the personal information. A goal of the policy shall be to reduce the risk of future breaches of the security of the system.

(b) Considerations.--In developing the policy, a Township contractor shall reasonably consider similar existing Federal policies and other policies, best practices identified by other states and relevant studies and other sources as appropriate in accordance with best practices as established by the Federal Government and the Commonwealth.

(c) Review and update.--The policy shall be reviewed at least annually by the Township contractor and updated as necessary.

**Section 11.** Compliance with Federal requirements. A Township contractor that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the Township contractor's primary state, shall be in compliance with this policy.

**Section 12.** The Board of Supervisors shall reexamine said policy from time to time and make updates, revisions and amendments to such policy by official resolution, as deemed necessary or convenient.