**NEW CASTLE FIRE DISTRICT NO. 1**
**DATA BREACH POLICY**

1. **Purpose**: The Policy's purpose is to make sure that personal, private information maintained by the Fire District in its information technology systems is properly protected, and that any system security breach that results in the disclosure or potential disclosure of private information will be reported to the affected persons or entities.

2. **Definitions**:

A. For purposes of this Policy, the following definitions shall apply:

(1) "Breach of the security of the system" shall mean the unauthorized acquisition, or acquisition without valid authorization, of computerized data, which compromises the security, confidentiality, or integrity of personal information maintained by a state entity.

(a) Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

(b) 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, such state entity may consider the following factors, among others:

(i) 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;

(ii) Indications that the information has been downloaded or copied; or

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

(2) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative non-profit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification.

(3) "Private information" shall mean either:

(a) Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element, or the combination of personal information plus the data element, is not encrypted, or encrypted with an encryption key, that has also been accessed or acquired:

(i) Social security number;

(ii) Driver's license number or non-driver identification card number;

(iii) Account number, credit or debit card number, in combination with any required security code, access code, password, or other information which would permit access to an individual's financial account;

(iv) Account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password;

(v) Biometric information (data generated by electronic measurements of an individual's unique physical characteristics) such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(vi) A username or e-mail address in combination with a password or security question that would permit online account access.

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

3. **Actions To Be Taken In The Event Of Breach**:

A. In the event that the Fire District owns or licenses computerized data that includes private information, it shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any New York resident whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

(1) The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of State Technology Law § 208, or any measures necessary to determine the scope of the breach and restore the integrity of the data system.

B. The Fire District shall consult with NYS Office of Information Technology Services to determine the scope of the breach and restoration measures. Within ninety (90)

days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system.

C. Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons.

(1) Such a determination must be documented in writing and maintained for at least five (5) years.

(2) If the incident affected over five hundred (500) residents of New York, the Fire District shall provide the written determination to the New York State Attorney General within ten (10) days after the determination.

D. If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this Policy shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the Department of State and the Office of Information Technology Services pursuant to New York State Technology Law § 208(7)(a), and to consumer reporting agencies pursuant to New York State Technology Law § 208(7)(b):

(1) Regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(2) Regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(3) Part 500 of Title 23 of the official compilation of codes, rules, and regulations of the state of New York, as amended from time to time; or

(4) Any other data security rules and regulations of, and the statutes administered by, any official department, division, commission, or agency of the federal or New York state government as such rules, regulations, or statutes are interpreted by such department, division, commission, or agency, or by the federal or New York state courts.

E. If the Fire District maintains computerized data that includes private information which such Fire District does not own, it 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, accessed or acquired by a person without valid authorization.

(1) The notification required by State Technology Law § 208 may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. In that case, the notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

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

(1) Written notice;

(2) Electronic notice:

(a) The person to whom notice is required must expressly consented to receiving said notice in electronic form.

(b) The Fire District must keep a log of each notification when it notifies affected persons in such form.

(c) In no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(3) Telephone notification, provided that a log of each such notification is kept by the Fire District when it notifies affected persons;

(4) Substitute notice, if the Fire District demonstrates to the New York State Attorney General that the cost of providing notice would exceed two hundred and fifty thousand dollars ($250,000.00), or that the affected class of subject persons to be notified exceeds five hundred thousand dollars (500,000.00), or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(a) E-mail notice when the Fire District has an e-mail address for the subject persons;

(b) Conspicuous posting of the notice on the Fire District's website; and

(c) Notification to major statewide media.

G. Regardless of the method by which notice is provided, such notice shall include:

(a) Contact information for the Fire District;

(b) The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention; and

(c) A description of the categories of information that were, or are reasonably believed to have been, accessed or 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 accessed or acquired.

H. In the event that any New York residents are to be notified, which shall be made without delay, the Fire District will notify the New York State Attorney General, the Department of State, and the State Office of Information Technology Services of the following:

(1) The timing, content and distribution of the notices;

(2) The approximate number of affected persons; and

(3) Provide a copy of the template of the notice sent to affected persons.

I. In the event that more than five thousand (5,000) New York residents are to be notified at one time, the Fire District shall also notify consumer reporting agencies 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 residents.

J. If the Fire District is required to provide notification of a breach, including breach of information that is not "private information" as previously defined, to the Secretary of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, it shall provide such notification to the New York State Attorney General within five (5) business days of notifying the Secretary of State.

4. **Amendment**: The Board of Fire Commissioners may amend this Policy from time to time in accordance with the law.

5. **Adoption**: This Policy is adopted on June 20, 2024 and supersedes any previous version.