ERIE COUNTY WATER AUTHORITY

Policy & Procedures for Data Security

Section 1: Purpose

The Erie County Water Authority (the "Authority") seeks to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information it collects from employees, customers and vendor and to establish a notification protocol in the event of a data breach.

Section 2: Definitions.

(a) The "Authority" means the Erie County Water Authority, a body corporate and politic constituting a public benefit corporation of the State of New York, whose formation and powers are set forth in Public Authorities Law §§ 1050-1073.

(b) "Personal Information" means any information concerning a natural person which because of name, number, personal mark or other identifier can be used to identify such natural person.

(c) "Private Information" is means Personal Information pertaining to residents of New York State in combination with a:

i. Social Security Number;
ii. Drivers' 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 or password or other information that would permit access to an individual's financial account;
iv. Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code or password;
v. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or

vi. A username ore e-mail address in combination with a password or security question and answer that would permit access to an online account.

(d) "Retention Schedule" means the Authority's Office Records Retention Schedule, as amended on February 13, 2013.

(e) "Record's Management Officer" means the Secretary to the Authority.

(f) "Division Heads" mean the Secretary to the Authority, the Authority's Chief Operating Officer, its Chief Financial Officer, and its General Counsel.

(g) "Department Heads" mean the Authority's Division Heads, the Authority's Director of Administration, its Comptroller, its Executive Engineer, and its Director of Water Quality.

Section 3: Collection of Private Information.

It is the policy of the Authority to collect Private Information for legitimate business purposes only and to ensure that collected information is safely destroyed when no longer needed or at the end of its retention period as outlined in the Retention Schedule.

The Record's Management Officer assisted by the Authority's Security Officer and Information Technology Department are primarily responsible for managing data security and retention. Division and Department heads are responsible for identifying Private Information collected and stored by its units, managing access, and guarding against unauthorized access to information.

Section 4: Safeguarding Data.

The Authority is obligated under Section 1125 of the New York State Public Health Law and America's Water Infrastructure Act of 2018 to periodically assess the vulnerability, risk and resiliency of its cybersecurity system. The intention of both Acts is to assess safeguards in the Authority's information technology infrastructure system and control risk from both external and internal security threats.

The Authority requires contractors, when appropriate, to acknowledge its compliance with all applicable data security and protection legislation and to carry an adequate amount of cybersecurity insurance.

The Authority has designated the Authority's Security Officer to annually review internal and external data security risks. Following this annual review, the

Authority has designated its General Counsel to review this Policy & Procedures for Data Security and update or revise this Policy as the circumstances dictate.

The Authority has designated the Director of Administration and the Comptroller to ensure all service providers handling Personal Information or Private Information have adequate security program practices and procedures. The Chief Financial Officer shall maintain an inventory of service providers who handle Personal Information or Private Information.

It is the policy of the Authority to ensure all new employees receive data security training, including a review of this policy. Periodic training for existing employees will be conducted by the Human Resources Department.

Section 5: Notification in the Event of a Data Breach

The Authority carries a substantial cyber insurance policy which, in the event Private Information is compromised, includes coverage for notification to impacted individuals; credit monitoring, credit freezing, and credit thawing; social media monitoring; password management services, and fraud alert services.

The Authority has designated that the Authority's Claims Representative/Risk Manager shall notify the Authority's insurance carrier in the event that Private Information has been compromised.

It is the policy of the Authority to assess any suspected data breach to determine whether Private information is in the possession of an unauthorized person, as well as whether it has been downloaded, copied or used by an unauthorized person. If a breach is confirmed, the Authority will comply with all applicable laws and regulations governing data security including notifying, if warranted, the affected individuals, the New York State Attorney General; the New York Department of State; the New York State Police; and Consumer Reporting Agencies. The assessment of any suspected data breach and determination of notification of same shall be made by the Authority's General Counsel.