RESOLUTION 18-013

RESOLUTION OF THE BOARD OF DIRECTORS OF THE SOUTH ADAMS COUNTY WATER AND SANITATION DISTRICT ACTING FOR ITSELF AND BY AND THROUGH ITS SOUTH ADAMS COUNTY WATER AND SANITATION DISTRICT ACTIVITY ENTERPRISE REGARDING DATA SECURITY

WHEREAS, the South Adams County Water and Sanitation District ("District") is a pre-1965 special district and political subdivision of the State of Colorado, acting pursuant to portions of the Colorado Special District Act, §§ 32-1-101, *et seq.*, C.R.S.

WHEREAS, the District has created, maintains, and in the provision of water and sanitary sewer service generally acts through its South Adams County Water and Sanitation District Activity Enterprise.

WHEREAS, in order to perform its governmental purposes, the District uses and retains paper and electronic documents containing personal identifying information of its customers and employees.

WHEREAS, the District has adopted the Colorado State Archivist's Records Retention Schedule and maintains additional protocols for records management (collectively, "Records Management Policy").

WHEREAS, in light of HB 18-1128 (codified as part 73 of Title 24, C.R.S. and hereinafter referred to as "Part 73"), which was enacted into law to provide additional protections against the harmful disclosure of personal identifying information, the District has determined to supplement its Records Management Policy by incorporating the provisions of Part 73.

WHEREAS, the Board finds that passage of this Resolution is reasonably related to District purposes and is in the best interests of the District, its residents, customers, and taxpayers.

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF SOUTH ADAMS COUNTY WATER AND SANITATION DISTRICT AS FOLLOWS:

1. "PII" or "Personal Identifying Information". Means a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in section 24-73-103 (1)(a); an employer, student, or military identification number; or a financial transaction device, as defined in section 18-5-701 (3), including, without limitation any instrument or device whether known as a credit card, banking card, debit card, electronic funds transfer card, or guaranteed check card, or account number representing a financial account or affecting the financial interest, standing, or obligation of or to the account holder, that can be used to obtain cash, goods, property, or services or to make financial payments.

2. "Personal Information." Means:
   a. a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: social security number; driver's license number or identification card number; student, military, or passport identification number; medical information; health insurance identification number; or biometric data, as defined in subsection (1)(a) of this section;
   b. a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or
   c. a Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
   d. "personal information" 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.

3. Incorporation of Part 73 into Records Management Policy. The District's Records Management Policy is hereby amended to incorporate the provisions of Part 73. In the event of any conflict or inconsistency between the Records Management Policy and Part 73, the provision which is more likely to prevent the unauthorized disclosure of PII shall control.

4. Specific Provisions. Without limiting the general incorporation of Part 73 into the Records Management policy in the prior Section, the District shall specifically:
   a. *Disposal of PII.* When paper or electronic documents containing PII have surpassed their retention period, are not subject to a legal hold, and are no longer needed, the District shall destroy or arrange for the destruction of such documents by shredding, erasing, or otherwise modifying the PII to make the PII unreadable or indecipherable through any means.
   b. *Protection of PII.* The District shall continue to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII and the nature and size of the District.
   c. *Protection of PII in the Possession of Third Parties.* The District shall require that third party service providers implement and maintain reasonable security procedures and practices consistent with Section 24-73-102(2), C.R.S.
   d. *Disclosure of Breach.*
      i. If the District becomes aware that a security breach may have occurred, it shall conduct in good faith a prompt investigation to determine the likelihood that personal information, as such term is defined in §24-73-103(1)(g)(I)(A), C.R.S., has been or will be misused. The District shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.

ii. Notice consistent with §§ 24-73-103(1)(f), (2)(b), & (c), C.R.S. must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

e. *Notice to the Attorney General.* Upon the discovery of a data breach, the District shall in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination, provide notice to the Colorado Attorney General if the security breach is reasonably believed to have affected 500 Colorado residents or more, unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur.

5. No Third Party Rights. This Resolution is not intended to and does not create any rights in parties for whom the District retains PII that are not otherwise provided by law.

6. Repeal and Ratification. All Resolutions and other prior acts of the Board inconsistent with this Resolution are hereby repealed to the extent of such inconsistency for the purposes of this Resolution, and all actions of the officers, agents and employees of the District which are in furtherance of or in conformance with the purposes and intent of this Resolution are hereby in all respects ratified, approved and confirmed.

Whereupon, a motion was made and seconded, and upon a majority vote this Resolution was approved by the Board.

ADOPTED AND APPROVED this 11th day of September, 2018.

SOUTH ADAMS COUNTY WATER AND SANITATION DISTRICT FOR ITSELF AND ON BEHALF OF ITS SOUTH ADAMS COUNTY WATER AND SANITATION DISTRICT ACTIVITY ENTERPRISE

President

ATTEST:

Secretary