

**RESOLUTION NO. 2018-12-4**

**RESOLUTION OF THE BOARD OF DIRECTORS OF THREE LAKES WATER AND  
SANITATION DISTRICT TO IMPLEMENT A PERSONAL DATA PROTECTION  
POLICY**

WHEREAS, Three Lakes Water and Sanitation District (“District”) is a special district and political subdivision of the State of Colorado, acting pursuant to certain powers set forth in the Colorado Special District Act, C.R.S. § 32-1-101, *et seq.*; and

WHEREAS, in the District’s ordinary course of business, it maintains, owns, and licenses limited amounts of personal identifying information and/or computerized data that include personal information; and

WHEREAS, the Colorado legislature recently enacted C.R.S. §§ 24-73-101, *et seq.*, which requires special districts to implement new data protection policies to prevent unauthorized use or disclosure of certain kinds of personal information within a district’s custody or control; and

WHEREAS, to comply with the new data protection requirements, the District desires to implement the following policies and practices to protect the data privacy of its customers and employees; and

WHEREAS, this Resolution establishes a policy for destroying personal identifying information owned, licensed or maintained by the District, implements security procedures and practices to protect the same kinds of data, and outlines a notice policy in the event that personal information is disclosed as a result of a security breach; and

WHEREAS, the Board of Directors of the District has determined that the policies and practices contained in this Resolution are reasonably designed to protect the data privacy of its customers and residents, given the nature of the data and the size of the District.

**NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF  
THE DISTRICT AS FOLLOWS:**

1. The Board hereby adopts the Personal Data Protection Policy set forth in **Exhibit A**, which is attached hereto and incorporated herein by reference.
2. The Personal Data Protection Policy is effective immediately upon execution of this Resolution.
3. The Board directs the District Manager to update the Personal Data Protection Policy, if needed, to comply with any amendments to statutes affecting the policy, including C.R.S. §§ 24-73-101, *et seq.*

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

ADOPTED this 10<sup>th</sup> day of December, 2018.

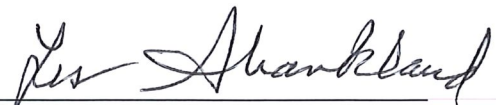
**THREE LAKES WATER AND SANITATION  
DISTRICT**



---

Matt Reed, Vice Chairperson

ATTEST:



---

Les Shankland, Secretary/Treasurer

## Exhibit A

### PERSONAL DATA PROTECTION POLICY

A. Definitions. For purposes of this Personal Data Protection Policy, the terms below have the meaning given to them in C.R.S. §§ 24-73-101, *et seq.*, and 18-5-701(3), both as amended. The following definitions are provided for convenience. In the event there is a conflict between a definition contained in this Policy and the corresponding definition in the statute, the statute controls.

1. "Biometric data" means "unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account."

2. "Financial Transaction Device" means any instrument or device whether known as a credit card, banking card, debit card, electronic fund transfer card, or guaranteed check card, 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, but shall not include a "check," a "negotiable order of withdrawal," and a "share draft" as defined in C.R.S. § 18-5-205. C.R.S. § 18-5-701(3).

3. "Personal Identifying Information" means a social security number, a personal identification number, a password, pass code, an official state or government-issued driver's license or identification card number, a government passport number, Biometric Data, an employer, student, or military identification number, or a Financial Transaction Device. C.R.S. § 24-73-101(4)(b).

4. "Personal Information" means:

- i) 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;
- ii) 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
- iii) A Colorado resident's account number, credit card or debit card number in combination with any required security code, access code, or password that would permit access to that account.

"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. C.R.S. § 24-73-103(1)(g).

5. “Security Breach” means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of Personal Information maintained by a governmental entity. Good faith acquisition of Personal Information by an employee or agent of a governmental entity for the purposes of the governmental entity is not a security breach if the Personal Information is not used for a purpose unrelated to the lawful government purpose or is not subject to further unauthorized disclosure. C.R.S. § 24-73-103(1)(h).

B. Destruction and Disposal Policy. The District shall promptly destroy or arrange for proper disposal of all paper and electronic records under its control or custody containing Personal Identifying Information when they are no longer needed by the District.

1. Physical Records. The District shall shred onsite and/or arrange for a qualified contractor to provide onsite or offsite destruction of all physical records and documents containing Personal Identifying Information. If the District contracts for disposal of physical records and documents containing Personal Identifying Information, the District shall require verification from the contractor that the records and documents were properly destroyed or disposed of as required by C.R.S. § 24-73-101(1).

2. Electronic Records. The District shall permanently erase or modify all electronically-stored records or data containing Personal Identifying Information to the point that the Personal Identifying Information is unreadable or indecipherable through any means. This District’s electronic records destruction policy applies to flash drives, CDs, hard-drives, etc., as well as data and records stored on the District’s network, server, cloud storage, etc.

C. Security Procedures. The District shall implement the following security procedures to prevent the unauthorized access, use, modification, disclosure or destruction of Personal Identifying Information under its control:

1. The District shall keep all records containing Personal Identifying Information in a secure location, either physically at the District’s office or in a password-protected or encrypted electronic format.

2. The District shall limit access to systems or files containing Personal Identifying Information to District employees or agents that require access to Personal Identifying Information in their official capacities. Employees or agents with access to Personal Identifying Information must respect the confidentiality of such information, and refrain from all careless or negligent conduct that might lead to unauthorized access, use, modification, disclosure or destruction of Personal Identifying Information.

3. District employees and agents are prohibited from sharing or disclosing Personal Identifying Information to any party without the District’s prior written consent. The District shall only give approval for disclosure or sharing of Personal Identifying Information when it is for a justified business necessity.

4. The District shall require that if Personal Identifying Information is disclosed to a third-party service provider in the course of the District’s business, the third-party service provider will implement and maintain reasonable security procedures and practices that are appropriate to the nature of the Personal Identifying Information disclosed by the District and

reasonably designed to help protect the Personal Identifying Information from unauthorized access, use, modification, disclosure or destruction.

5. In the event of a Security Breach, the District shall cooperate with law enforcement and work promptly to restore the integrity of the District's computerized systems containing Personal Identifying Information and/or Personal Information and comply with Section D.

D. Notification of a Security Breach.

1. Investigation. As soon as the District becomes aware that a Security Breach may have occurred, the District shall conduct a good faith and prompt investigation to determine if any Personal Information was misused or is reasonably likely to be misused. Depending on the severity of the Security Breach, the District may contract with a data security consultant to assist in the investigation.

2. Notice. As expediently as possible and without unreasonable delay, and no later than thirty days from the determination that a Security Breach has 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, the District shall provide all affected Colorado residents with notice of the Security Breach, unless the District's investigation determines that no Personal Information was misused, and misuse is reasonably likely not to occur.

i) Any notice provided by the District will contain the information required by C.R.S. § 24-73-103(2)(b). If the Security Breach includes email account log-in credentials, the District will provide notice to affected Colorado residents by an uncompromised means of communication defined in C.R.S. § 24-73-103(1)(f).

ii) In addition to providing the required notice, the District shall direct affected Colorado residents to change their password, security questions and answers, or other security features that were affected by the Security Breach and all other online accounts that share the same username, email, password, or other security features to prevent further disclosure of Personal Information.

3. Additional Notice Requirements. In addition to the notice described above, depending on the size and scope of the Security Breach, the District will provide the following additional notices 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:

i) If it is reasonably believed that the Security Breach affected 500 Colorado residents or more, the District shall provide notice to the Colorado attorney general pursuant to C.R.S. § 24-73-103(2)(k)(I).

ii) If the District is required to notify more than 1,000 Colorado residents, the District shall provide notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the

federal “Fair Credit Reporting Act,” 15 U.S.C. § 1681a(p), of the anticipated date of the notice sent to Colorado residents and the approximate number of residents who will be notified.

4. Security Breach of Encrypted Information. The District will comply with all investigation and notice requirements described above if encrypted data containing Personal Information and the corresponding encryption key or other means of deciphering that data is part of a Security Breach.

5. Breach of a Third-Party Service Provider. The District shall post notice on the homepage of its website if it receives notice that a third-party service provider of the District suffered a Security Breach containing Personal Information from the District’s customers. The District shall also cooperate with the third-party service provider to resolve the security issue.

**Adopted December 10, 2018.**