SOUTH METRO FIRE RESCUE FIRE PROTECTION DISTRICT

RESOLUTION NO. 2018-06

A RESOLUTION ADOPTING THE PROTECTIONS FOR CONSUMER DATA PRIVACY POLICY

WHEREAS, the South Metro Fire Rescue Fire Protection District of the Counties of Douglas and Arapahoe, Colorado (the "District") is a quasi-municipal corporation and political subdivision of the State of Colorado; and

WHEREAS, pursuant to Sections 32-1-1001(1)(h-i), C.R.S., the Board of Directors of the District ("Board") is responsible for the management, control, and supervision of all business and affairs of the District;

WHEREAS, the Colorado Legislature recently passed the "Protections for Consumer Data Privacy" Act, H.B. 18-1128 ("Act"), which requires governmental entities in Colorado to develop a written policy for the destruction and proper disposal for paper and electronic documents that contain personal identifying information, to maintain reasonable security procedures for personal identifying information, and to notify Colorado residents following a security breach; and

WHEREAS, to comply with the Act, the Board desires to supplement its Colorado Open Records Act Policy and adopt and implement a policy for the destruction and proper disposal for paper and electronic documents that contain personal identifying information, a policy for protecting personal identifying information from security breaches, and a policy for notifying Colorado residents following a security breach.

NOW, THEREFORE, BE IT RESOLVED by the Board of Directors of the South Metro Fire Rescue Fire Protection District as follows:

Section 1. Definitions.

(a) "Personal Identifying Information" means the following:
- i. Social security number
- ii. Personal identification number
- iii. A password
- iv. A pass code
- v. An official state or government-issued driver's license or identification card
- vi. A government passport number
- vii. Biometric data, as defined in C.R.S. § 6-1-716(1)(a)
- viii. An employer, student, or military identification number
- ix. A financial transaction device, as defined in C.R.S. § 18-5-701

(b) "Third Party Service Provider" means an entity that has been contracted to maintain, store, or process personal information on behalf of the District.

Section 2. Security Measures. The District shall protect Personal Identifying Information from unauthorized access, use, modification, disclosure, or destruction by implementing and maintaining reasonable security procedures and practices. Such procedures and practices shall include but not be limited to:

(a) limiting access to Personal Identifying Information by individuals to the minimum level of information necessary to accomplish their responsibilities by requiring password access to workstations, servers, applications, parts of applications;

(b) modifying an individual's access to Personal Identifying Information when the individual's job responsibilities change, new or upgraded application software allows greater control of application access, or the individual's association with the District has been terminated;

(c) monitoring system logins, file access, and security incidents associated with Personal Identifying Information stored on or transmitted by the District's computer systems, including:

  i. Using and regularly reviewing system traces;

  ii. Using and regularly reviewing audit functionality available through application software; and

(d) ensuring that appropriate education and procedures are in place and enforced so that the District's board directors, employees, volunteers, committee members, and agents are trained properly regarding privacy and confidentiality in accordance with the District's policies and the applicable laws and regulations.

Section 3. Document Destruction and Disposal. The District's board of directors, employees, volunteers, committee members, and agents are required to comply with the following rules:

(a) When paper or electronic documents contain Personal Identifying Information, and such paper or electronic documents are no longer needed, unless longer retention is required by contractual or legal requirements, the District shall destroy or arrange for the destruction of such paper or electronic documents within its custody or control by shredding, erasing, or otherwise modifying the Personal Identifying Information in the paper or electronic documents to make the Personal Identifying Information unreadable or indecipherable through any means;

(b) All electronic documents containing Personal Identifying Information that are no longer needed and are not required by law to be retained shall be deleted from all computers, data bases, networks, and back-up storage;

(c) No paper or electronic documents containing Personal Identifying Information will be destroyed if pertinent to any ongoing or anticipated government investigation or proceeding or litigation;

(d) No paper or electronic documents containing Personal Identifying Information will be destroyed if their retention or destruction is additionally governed by other laws of the State or the Federal Government;

(e) If there is any question as to whether or not a document contains Personal Identifying Information, it should be treated as if it does include Personal Identifying Information and should be destroyed.

Section 4. Third Party Service Providers. If the District contracts with a third party service provider to maintain, store, or process Personal Identifying Information on behalf of the District, the third party service provider will be required to implement and maintain reasonable security procedures and practices that are:

(a) appropriate to the nature of the Personal Identifying Information that is disclosed to the third party service provider; and
(b) reasonably designed to help protect the Personal Identifying Information from unauthorized access, use, modification, disclosure, or destruction.

Section 5. Discovery of Security Breach. After the District learns that a security breach may have occurred, the District will promptly conduct in good faith an investigation to determine the likelihood that personal information of Colorado residents has been or will be misused.

Section 6. Notice Required. The District will give notice to the affected residents within thirty (30) days of learning of the breach if the District determines that the misuse of information has occurred or is reasonably likely to occur. The District will provide notice to the affected residents by one or more of the methods listed in C.R.S. § 24-73-103(1)(f). If the District is required to give notice, the notice shall include the following:

(a) Date, estimated date, or estimated date range of the security breach;
(b) A description of the Personal Identifying Information that was acquired or reasonably believed to have been acquired;
(c) Information that the individual can use to contact the District about the breach;
(d) Toll-free numbers, addresses, and websites for consumer reporting agencies;
(e) Toll-free number, address, and website for the federal trade commission; and
(f) A statement that the individual can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

If the District is required to give notice, the District shall also direct the resident to change his/her password, security question or answer, and take any other applicable steps to protect his/her online account with the District and all other online accounts for which the resident uses the same user name, email address, password, and/or security question or answer.

The District will not charge the affected Colorado residents for complying with these notice requirements.

Section 7. Additional Notice Requirements.

(a) If the District is required to notify five hundred (500) Colorado residents or more, the District will notify the Colorado Attorney General within thirty (30) days after the date of determination that a breach has occurred.
(b) If the District is required to notify more than one thousand (1000) Colorado residents of a security breach, the District will immediately notify all consumer

reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of notification to the residents and the approximate number of residents to be notified.

Section 8. Colorado Open Records Act. The purpose of this Resolution is to supplement and not replace the District's Colorado Open Records Act Policy and Records Retention Policy and therefore this Resolution shall be read in conjunction with the requirements of the same.

Section 9. Effective Date. The provisions of this Resolution shall take effect as of the date set forth below.

Approved and adopted this 15th day of August, 2018.

SOUTH METRO FIRE RESCUE
FIRE PROTECTION DISTRICT

By: _____
Laura Simon, President

ATTEST:

By: _____
Ronda Scholting, Secretary