

**RESOLUTION OF THE  
BOARD OF DIRECTORS OF LEGACY PARK PUBLIC IMPROVEMENT  
AUTHORITY**

**A RESOLUTION ADOPTING PROCEDURES FOR PROTECTING AND DESTROYING  
CUSTOMER INFORMATION MAINTAINED BY THE AUTHORITY**

**WHEREAS**, the Legacy Park Public Improvement Authority (the “Authority”) was formed pursuant to the Legacy Park Public Improvement Establishment Agreement dated April 27, 2026 entered into among Legacy Park Metropolitan District Nos. 1 – 5 (the “Establishment Agreement”), in accordance with Section 29-1-203, C.R.S., and in conformity with Section 29-1-203.5, C.R.S.; and

**WHEREAS**, the Board of Directors of the Authority (the “Board”) has a duty to perform certain obligations in order to assure the efficient operation of the Authority; and

**WHEREAS**, pursuant to Section 2.10 and Section 3.01(i) of the Establishing Agreement, the Board has the power to adopt, modify, and amend bylaws and regulations; and

**WHEREAS**, on May 29, 2018, House Bill (“HB”) 18-1128 was signed into law requiring governmental entities in Colorado that maintain, own, or license personal identifying information 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 and practices for personal identifying information, and to notify Colorado residents following a security breach of personal information, as set forth in §§ 24-73-101 *et seq.*, C.R.S.; and

**WHEREAS**, to comply with the provisions of HB 18-1128, the Board desires to 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, and a policy for notifying Authority Customers (as defined herein) following a security breach of personal information.

**NOW, THEREFORE**, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF LEGACY PARK PUBLIC IMPROVEMENT AUTHORITY AS FOLLOWS:

**Section 1.**     Definitions.

- (a) “Authority Customers” shall mean Colorado residents and any other individuals that have provided Personal Identifying Information and Personal Information to the Authority and such Personal Identifying Information and Personal Information is maintained by the Authority.
- (b) “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. § 24-73-103(1)(a)
  - viii. An employer, student, or military identification number
  - ix. A financial transaction device, as defined in C.R.S. § 18-5-701(3).
- (b) "Personal Information" means:
- (i) An Authority Customer'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 Authority Customer, 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 C.R.S. § 24-73-103(1)(a);
  - (ii) An Authority Customer'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) An Authority Customer'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.
- (c) "Security Breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of Personal Information maintained by the Authority.
- (d) "Third-Party Service Provider" means an entity that has been contracted to maintain, store, or process Personal Identifying Information or Personal Information on behalf of the Authority.

**Section 2.** Security Measures. The Authority shall protect Personal Identifying Information from unauthorized access, use, modification, disclosure, or destruction by implementing and maintaining the following security procedures and practices:

- (a) The Authority will limit access to Personal Identifying Information by the Authority's board of directors, employees, volunteers, committee members, and agents (collectively, the "Authority Associates") to the minimum level of information necessary to accomplish their duties and responsibilities by requiring password access to workstations, servers, applications, and certain parts of applications;
- (b) The Authority will modify or terminate an Authority Associate's access to Personal Identifying Information as necessary when the Authority Associate's duties and responsibilities change, new or upgraded application software allows greater

control of application access, or the Authority Associate's association with the Authority is terminated;

- (c) The Authority will monitor system logs, file access, and security incidents associated with Personal Identifying Information stored on or transmitted by the Authority's computer systems, including:
  - i. Using and regularly reviewing system traces;
  - ii. Using and regularly reviewing audit functionality available through application software; and
- (d) The Authority will educate the Authority Associates regarding privacy and confidentiality of Personal Identifying Information in accordance with these policies and the applicable laws and regulations.

The Authority may implement additional security procedures, as the Authority deems necessary, that are appropriate to the nature of the Personal Identifying Information and the nature and size of the Authority and its operations.

**Section 3.** Document Destruction and Disposal. The Authority is required to comply with the following rules:

- (a) When paper or electronic documents that contain Personal Identifying Information are in the custody or control of the Authority, and such paper or electronic documents are no longer needed, unless longer retention is required by contractual or legal requirements, the Authority shall destroy or arrange for the destruction of such paper or electronic documents 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) No paper or electronic documents containing Personal Identifying Information will be destroyed if pertinent to any ongoing or anticipated government or law enforcement investigation or proceeding, or litigation;
- (c) 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; and
- (e) If there is any question as to whether a document contains Personal Identifying Information, the Authority shall consult with legal counsel for a final determination as to whether the document should be retained or destroyed.

**Section 4.** Third-Party Service Providers. Unless the Authority agrees to provide its own security protection for the Personal Identifying Information it discloses to a Third-Party Service Provider, the Authority shall require that the Third-Party Service Provider 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.** Disclosure of Security Breach. When the Authority becomes aware that a Security Breach may have occurred, the Authority will conduct, in good faith, a prompt investigation to determine the likelihood that Personal Information maintained by the Authority has been or will be misused.

- (a) Notice of Security Breach. Unless the Authority’s investigation determines that the misuse of information about Authority Customers has not occurred and is not reasonably likely to occur, the Authority shall give notice (“Notice”) to the affected Authority Customers in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a Security Breach occurred, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. The Authority shall not charge the Authority Customers for the cost of sending the Notice.
  - (1) Notice shall be provided by one of the following means:
    - (i) Written notice to the postal address listed in the records of the Authority;
    - (ii) Telephonic Notice;
    - (iii) Electronic Notice, if a primary means of communication by the Authority with an Authority Customer is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the federal “Electronic Signatures in Global and National Commerce Act”, 15 U.S.C. sec. 7001 *et seq.*; or
    - (iv) Substitute Notice, if the Authority determines that the cost of providing Notice will exceed \$250,000, the affected class of persons to be notified exceeds 250,000 persons, or the Authority does not have sufficient contact information to provide Notice. Substitute Notice shall be provided via e-mail if the Authority has e-mail addressed for the persons affected or via the conspicuous posting of the notice on the website page of the Authority.
  - (2) The Notice shall include, but need not be limited to, the following information:
    - (i) The date, estimated date, or estimated date range of the Security Breach;
    - (ii) A description of the Personal Information that was acquired or reasonably believed to have been acquired as part of the Security Breach;
    - (iii) Information that the Authority Customer can use to contact the Authority to inquire about the Security Breach;

- (iv) The toll-free numbers, addresses, and websites for consumer reporting agencies;
  - (v) The toll-free number, address, and website for the federal trade commission; and
  - (vi) A statement that the Authority Customer can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.
- (b) Additional Notice Upon Determination of Security Breach. If an investigation by the Authority determines that Personal Information as defined in subsection (1)(b)(ii) above has been misused or is reasonably likely to be misused, the Authority shall, in addition to the Notice set forth in subsection (5)(a) above, and in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a Security Breach occurred, and consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system, direct the person whose Personal Information as defined in subsection (1)(b)(ii) above has been breached to (i) promptly change his or her password and security question or answer, as applicable, or (ii) take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose Personal Information has been breached uses the same username or e-mail address and password or security question or answer.
- (c) Third-Party Service Providers. If the Authority uses a Third-Party Service Provider to maintain computerized data that includes Personal Information, the Authority shall require the Third-Party Service Provider to give notice to and cooperate with the Authority in the event of a Security Breach that compromises such computerized data, including notifying the Authority of any Security Breach in the most expedient time and without unreasonable delay following discovery of a Security Breach, if misuse of Personal Information about an Authority Customer occurred or is likely to occur. Cooperation includes sharing with the covered entity information relevant to the Security Breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.
- (d) Delayed Notice. The Authority may delay providing Notice as required by this Section 5 to affected Authority Customers if a law enforcement agency determines that Notice will impede a criminal investigation and the law enforcement agency has notified the Authority not to send Notice. The Authority will provide Notice in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the law enforcement agency determines that notification will no longer impede the investigation, and has notified the Authority that it is appropriate to send Notice.
- (e) Notice to the Colorado Attorney General. The Authority shall provide notice of any Security Breach to the Colorado Attorney General in the most expedient time

possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a Security Breach occurred, if the Security Breach is reasonably believed to have affected five hundred (500) Authority Customers or more, unless the investigation determines that the misuse of information about Authority Customers has not occurred and is not likely to occur.

- (f) Notification to Consumer Reporting Agencies. If the Authority is required to notify more than one thousand Authority Customers of a Security Breach pursuant to this Section 5, the Authority shall also notify, in the most expedient time possible and without unreasonable delay, 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. sec. 1681a (p), of the anticipated date of the notification to the Authority Customers and the approximate number of Authority Customers who are to be notified.

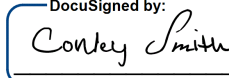
**Section 6.** Colorado Open Records Act. This Resolution is intended to supplement and not replace the Authority's Colorado Open Records Act Policy and/or Records Retention Policy, if adopted by the Authority, and therefore this Resolution shall be read in conjunction with the requirements of the same.

**Section 7.** Effective Date. This Resolution shall take effect on the date and at the time of its adoption and shall remain effective until otherwise supplemented or amended by the Board.

*(Signature Page Follows.)*

ADOPTED AND APPROVED THIS 24TH DAY OF AUGUST, 2026.

LEGACY PARK PUBLIC IMPROVEMENT  
AUTHORITY

By:   
E3FE24C883FA468...  
Conley Smith, President

*(Signature Page to the Legacy Park Public Improvement Authority Resolution Adopting Data Protection Policy)*