RESOLUTION OF CASTLE VALLEY RANCH TOWNHOMES ASSOCIATION, INC. ADOPTING A POLICY REGARDING THE PROTECTION OF PERSONAL IDENTIFYING INFORMATION

SUBJECT: Adoption of a policy regarding how personal identifying information of Owners shall be protected, as the Association is an entity that maintains personal identifying information in the course of its business.

PURPOSE: To establish uniform procedures for the storage and protection of Owners' personal identifying information.

AUTHORITY: The Association's Declaration, Articles of Incorporation, Bylaws, and pursuant to C.R.S. § 6-1-713.

EFFECTIVE DATE: January 10th, 2024

RESOLUTION: Castle Vally Ranch Townhomes Association, Inc. ("Association") hereby adopts the following Policy regarding the storage and protection of Owners' personal identifying information ("PII"):

1. **Definitions.**
   a. "Personal Identifying Information" or "PII"
      i. Includes any of the following:
         1. Social security number;
         2. Personal identification number (Pin #);
         3. Password;
         4. Pass code;
         5. Official state or government-issued driver's license or identification card number;
         6. Government passport number;
         7. Biometric data (i.e., fingerprints), as defined in C.R.S. 24-73-103(1)(a);
         8. Employer, student, or military identification number; or
         9. Financial transaction device (credit card, banking card, or debit card information), as defined in C.R.S. 18-5-701(3).
      ii. Does NOT include:
         1. Checks;
         2. Negotiable orders of withdrawal; or
         3. "Share drafts."

   b. "Third-party Service Providers" are entities that have been contracted to maintain, store, or process personal information on behalf of the Association.

   c. Other Definitions. All other capitalized terms shall have the same meaning as set forth in the Association's Declaration.

2. **Collection of PII.** The Association will only obtain and store PII provided by the Owner. PII obtained and stored by the Association is generally limited to usernames and passcodes for the Association's website, credit card numbers, and bank account information. The Association shall not obtain or store an Owner's social security number, date and/or place of birth, driver's license number, passport number, or any biometric information as a standard practice.

3. **Access to PII.** Access to PII shall be limited to the Board of Directors ("Board") and agents & employees of the Association, which may include a management company employed by the Association and the Association's legal counsel, if any.

4. **Storage of PII.**

   a. Electronic Records. To protect against unauthorized access by third parties, all electronic files that contain PII shall be stored on secure servers or other secure electronic storage systems.

   b. Physical Records. All physical files that contain PII shall be stored within a locked file cabinet or room when not being actively viewed or modified.

   c. Third-party Service Providers. Any third-party service provider used to protect or store PII must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII involved and reasonably designed to help protect the PII from unauthorized access, use, modification, disclosure, or destruction.

5. **Transfer of PII.** Except for Owner requested login and password recovery for the Association's website, PII shall not be sent through any form of insecure electronic communication such as e-mail or instant messaging systems.

6. **Destruction of Records containing PII.** Electronic documents or paper documents containing personal identifying information must be destroyed by shredding, erasing, or otherwise modifying the personal identifying information rendering the personal identifying information unreadable or indecipherable through any means. The Association may contract with third party vendors to ensure the proper shredding of paper documents and the secure deletion of PII from computer servers or other electronic storage systems.

7. **Notification of Security Breach of PII.** The Board shall conduct a prompt investigation if at any time it believes that unauthorized access to PII has occurred. In the event of a breach, it shall notify the Owner(s) within thirty (30) days and provide specific information as to the nature of the breach, including a description of the PII that was accessed and the date of the breach.

8. **Supplement to Law.** The provisions of this Policy shall be in addition to and in supplement of the terms and provisions of the Declaration and the laws of the State of Colorado governing the Association.