

**POLICY REGARDING DISPOSAL OF PERSONAL IDENTIFYING
INFORMATION**

Purpose: Adoption of a policy regarding the disposal of Personal Identifying Information by the Town & Country Village Homeowners Association, Inc. ("Association").

Authority: §6-1-713, C.R.S.

Effective Date: March 21, 2019

Resolution: The Association hereby adopts the following policy:

1. The Association maintains paper and/or electronic documents that contain Personal Identifying Information (defined below) ("PII").
2. "Personal Identifying Information" consists of one or more of the following: social security number, a personal identification number, password, driver's license or i.d. card, employer, student or military identification number or financial account information.
3. The Association will implement and maintain reasonable security procedures and practices regarding PII.
4. When the Association no longer needs the paper and/or electronic documents containing the PII, such as when a homeowner ceases being an owner of property within the Association, the paper documents within its custody or control shall be shredded or delivered to a third party shredding contractor and the electronic documents containing the PII shall either be erased or the PII made permanently unreadable.
5. "Personal Information" consists of 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:
 - a. Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data;
 - 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.
6. "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.
7. If the Association becomes aware that a security breach consisting of unauthorized access compromising the confidentiality, security or integrity of Personal Information may have occurred, it will conduct a prompt investigation to determine the likelihood that personal information has been or will be misused.
 - a. The Association will provide notice to the affected owners not later than thirty days after the date of determination a security breach occurred.
 - b. "Notice" means:
 - i. Written notice to the postal address listed in the records of the Association;
 - ii. Telephonic notice;
 - iii. Electronic notice, if a primary means of communication by the Association with a Colorado resident 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 Association required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the covered entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:
 1. E-mail notice if the covered entity has e-mail addresses for the members of the affected class of Colorado residents;
 2. Conspicuous posting of the notice on the website page of the covered entity if the covered entity maintains one; and
 3. Notification to major statewide media.
 - c. Such notice shall include:
 - 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 resident can use to contact the Association 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 resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.
- d. If the Association determines that 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 has been misused or is reasonably likely to be misused, then the Association shall, in addition to the notice described above:
- i. Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the covered entity 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.
 - ii. For log-in credentials of an e-mail account furnished by the Association, the Association shall not comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined above or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the Association knows the resident customarily accesses the account.
 - iii. The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher

the secured information was also acquired in the security breach or was reasonably believed to have been acquired.

- e. The Association is prohibited from charging the cost of providing such notice to individual owners but must be included as a common expense.
- 8. If the Association is required to notify more than 500 Colorado residents, the Association must also notify the Attorney General within 30 days unless the investigation determines that misuse of the information has not occurred and is not likely to occur.
- 9. If the Association is required to notify more than 1,000 residents of a security breach as described above, the Association must also notify all consumer reporting agencies.

10. Supplement to Law

The provisions of this Resolution shall be in addition to and in supplement of the terms and provisions of the Declaration and the law of the State of Colorado governing the community.

11. Deviations

The Board may deviate from the procedures set forth in this Resolution if its sole discretion such deviation is reasonable under the circumstances.

12. Amendment

This policy may be amended from time to time by the Board of Directors.

13. Severability

Invalidation of one of the foregoing provisions by court order or judgment shall have no effect on the remaining provisions which shall remain in full force and effect.

Certification:

The undersigned *President* of the Board of Directors for Town & Country Village Homeowners Association, Inc., a Colorado nonprofit corporation, hereby certifies that the foregoing Resolution was approved and adopted by the Board of Directors of the Association, at a duly called and held meeting of the Board of Directors on *March 21*, 2019 to be effective *March 21*, 2019.

**Town & Country Village Homeowners
Association, Inc.**

Sue Leonard

By:
Its: