

CENTENNIAL GLEN HOMEOWNERS ASSOCIATION

RESOLUTION # 2020-12 FOR THE ADOPTION OF PROCEDURES FOR INFORMATION SECURITY AND DATA BREACH POLICY

EFFECTIVE DATE: May 19, 2020

Pursuant to the Colorado Common Interest Ownership Act (CCIOA), Declaration, Articles of Incorporation and the Bylaws of the Association, the Board of Directors hereby adopts the following procedures regarding information security and data breach policy.

Purpose: The policy is created to establish guidelines to be followed in compliance with the requirements of HB 18-1128 regarding consumer data privacy as codified at C.R.S. §§ 6-1-713, -713.5, and -716 (2018).

Policy:

Part I. Scope & Applicability

This policy applies to the use, storage, protection, and disposal of certain data owned, licensed, or maintained by the Association business or interact with internal networks and business systems, whether owned or leased by Association, an employee, or a third party.

This policy applies to Board Members, employees, contractors, consultants, temporaries, and others at the Association, including all personnel affiliated with third parties.

Part II. Disposal of Personal Identifying Information

- 2.1 Definitions. For the purpose of Part II of this Policy, the following definitions apply:
 - a. "Personal Identifying Information" or "PII" means a social security number; a personal identification number; a password; a 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.
- 2.2 To the extent the Association maintains paper or electronic documents during the course of its business that contain PII, the Association shall

destroy or arrange for the destruction of such paper and electronic documents containing PII when such PII is no longer needed, by shredding, erasing, or otherwise modifying the personal identifying information in the paper or electronic documents to make the PII unreadable or indecipherable through any means.

- 2.3 By way of example, the following types of information, which are commonly held by community associations would constitute PII
- a. Credit card numbers;
 - b. Information for processing Automated Clearing House (a/k/a "ACH") transactions; or
 - c. Passwords for accessing an Association website

Part III. Protection of Personal Identifying Information

- 3.1 To protect PII, as defined in section 2.1(a) of this Policy, from unauthorized access, use, modification, disclosure, or destruction, the Association shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII, as well as the nature and size of the Association's operations.
- 3.2 At minimum, the reasonable security measures implemented to protect PII shall include the following:
- a. Any paper records containing PII must be stored in an enclosed, locked area accessible only by authorized parties.
 - b. All computing devices used to store PII must be password protected and each authorized user must have their own unique password for the purpose of accessing the PII.
 - c. If the Association's PII is stored on a computer network, the network must be password protected.

Part IV. Notification of Security Breach

- 4.1 Definitions. For the purpose of Part IV of this Policy,
- a. "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 unencrypted data elements relating to the resident:
 - 1. Social security number;
 - 2. Student, military, or passport identification number;
 - 3. Driver's license number;

4. Identification card number;
 5. Medical information;
 6. Health insurance information; or
 7. Biometric data.
- ii. A Colorado resident's username or email 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 or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
- b. "Security Breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of Personal Information maintained by the Association.
- 4.2 If the Association becomes aware that a Security Breach may have occurred, it shall promptly conduct a good-faith investigation to determine the likelihood that Personal Information has been or will be misused. Unless the investigation determines that there has been no misuse of such Personal Information – and such misuse is not reasonably likely to occur – the Association shall provide notice to the affected parties in the most expedient time possible, but no later than 30 days after the date on which the Association had sufficient evidence to conclude a security breach took place.
- 4.3 The notice required by section 4.2, directly above, shall be in accordance with C.R.S. § 6-1-716 (as amended).

Part V. Third Party Service Providers

- 5.1 The term "Third-Party Service Provider" means an entity that has been contracted to maintain, store, or process PII, as defined in section 2.1 of this Policy, or Personal Information, as defined in section 4.1(a) of this Policy, on behalf of a covered entity. For example, most community management companies and or accountants would constitute Third Party Service Providers.
- 5.2 To protect PII, the Association shall require that its Third-Party Service Providers (i.e. management companies or accountants) implement and maintain reasonable security practices and procedures that are appropriate

to the nature of the PII disclosed to the Third-Party Service Provider and reasonably designed to help protect the PII from unauthorized access, use, modification, disclosure, or destruction.

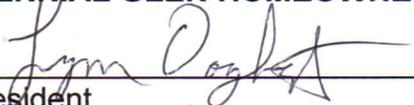
- 5.3 At a minimum, the Association's Third-Party Service Providers' security practices and procedures for protection of PII must meet the requirements set forth for the Association in section 3.2 of this Policy.
- 5.4 The Association shall require that if a Third-Party Service Provider becomes aware of a possible Security Breach, as defined in section 4.1(b) of this Policy, affecting the Association's data, the Third-Party Service Provider shall promptly notify the Association of the potential Security Breach.

Part VI. Miscellaneous

- 5.1 Definitions. Terms that are not defined in this policy are used as defined in C.R.S. §§ 6-1-713, -713.5, or -716. Additionally, initially capitalized or terms defined in the Declaration shall have the same meaning herein.
- 5.2 Failure of the Association to comply with any provision in this Policy shall not be deemed a defense to violation of any covenant, policy, or rule, including, but not limited to, nonpayment of assessments or other amounts.
- 5.3 If a court of competent jurisdiction finds any provision of this Policy to be unenforceable, the other provisions shall remain in full force and effect.
- 5.4 Deviations. The Board may deviate from the procedures set forth in this resolution if in its reasonable discretion such deviation is appropriate under the circumstances.
- 5.5 Amendment. This Procedure may be amended from time to time by the Board of Directors,

PRESIDENT'S CERTIFICATION: The undersigned, being the President of the Association, certifies that the foregoing Policy was adopted by the Board of Directors of the Association, at a duly called and held meeting of the Board of Directors on May 19, 2020 and in witness thereof, the undersigned has subscribed his/her name.

CENTENNIAL GLEN HOMEOWNERS ASSOCIATION, INC.

By: 
Its: President

Attested By its:  HOA Secretary