C.D.S. HOMEOWNERS ASSOCIATION, INC.
(dba YOSEMITE VILLAGE HOMEOWNERS ASSOCIATION)
POLICY FOR MAINTAINING, DESTRUCTION AND DISPOSAL OF PERSONAL IDENTIFYING INFORMATION AND NOTIFICATIONS OF SECURITY BREACHES

Adopted January 15, 2019

A. Application of Policy

This Policy for Maintaining, Destruction and Disposal of Personal Identifying Information and Notifications of Security Breaches ("PII Policy") sets forth the C.D.S. Homeowners Association, Inc. ("Association") policy for maintaining, destruction and disposal of personal identifying information ("PII"). All employees, staff, board members, officers, managers and contractors of the Association who have access to PII are required to adhere to this PII Policy.

B. Definitions

1. "Personal identifying information" the means any of the following:
    - social security number;
    - personal identification number;
    - password;
    - pass code;
    - official state or government-issued driver's license or identification card number;
    - government passport number;
    - biometric data;
    - employer, student, or military identification number; or
    - financial transaction device.

2. "Financial transaction device" means any instrument or device whether known as credit card; banking card; debit card; electronic fund transfer card; guaranteed check card; or account number representing a financial account or affecting the financial interest, standing, or obligation of or to the account holder, that can be used to obtain cash, goods, property, or services or to make financial payments. This does *not* include a check.

C. Policy

It is the Association's policy to protect the privacy of PII that is within Association's control. In furtherance of this policy, this PII Policy sets out the Association's intent to implement and maintain reasonable security procedures and practices to protect PII, as well as procedures for the destruction and proper disposal of PII when such PII is no longer needed by the Association.

D. Protection and Handling of PII

The following requirements apply to PII in paper records, electronic records and in oral communications, as well as any aggregation of PII in an electronic format (e.g., databases, webpages, e-mail, spreadsheets, tables, and file sharing services)

1. General. In addition to complying with all applicable legal requirements, the Association further limits the collection, use, disclosure, transmission, storage and/or disposal of PII to that which is necessary to allow the Association to fulfill its obligations to its members.

2. Collection. Collection of PII should be minimized.

3. Minimization. All employees, staff, board members, officers, managers and contractors of the Association are responsible for minimizing the use of PII and minimizing aggregations of PII. The risk of unauthorized disclosure of or access to PII increases with the amount of data. The number and scope of physical and electronic copies and repositories of PII should be kept to the minimum necessary and only for the time period where a valid business need for the information exists.

4. Transmission of PII. The transmission of PII should be minimized. If the transmission of PII is necessary, PII may not be transmitted to external parties outside the Association (e.g. via mail, fax, e-mail, instant messaging) without appropriate security controls. Great care is taken to ensure that e-mails are sent only to intended recipients.

5. Access to Association Files. The Association will seek to maintain its files and documents that may contain PII with its management company. In the event the Association maintains files or documents that may contain PII in a location other than with its management company, any physical files or documents will be maintained in the home or office of an officer of the Association, segregated from personal files or documents, and not accessible by the general public. Any electronic files will be maintained in locations secured by passwords. Electronic files that contain PII will not be accessed using unsecured wifi networks.

6. Permitted Disclosure to Third-Party Service Providers. All employees, staff, board members, officers, managers and contractors of the Association may release PII to third-party service providers only as permitted by law/regulation and this PII Policy. Third-party service providers to whom the Association employees, staff, board members, officers, managers and contractors are disclosing PII must be bound by agreements with appropriate PII safeguarding and use provisions pursuant to C.R.S. 6-1-713.5(2).

E. Destruction and Disposal

1. General. When physical or electronic PII documents are no longer needed, the Association will destroy, or arrange for the destruction of such PII documents by shredding, erasing or otherwise modifying the PII to make the PII unreadable or indecipherable through any means.

2. Destruction. Approved disposal methods include:
   a. Physical PII documents shall be disposed of by one (or a combination) of the following methods: documents shall be shredded using cross-cut shredders; or disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor.
   b. Electronic PII files (*e.g.*, physical disks, flash drives, hard-drives, etc.) shall be disposed of by one of the following methods: overwriting magnetic media (overwriting uses a program to write binary data sector by sector onto the media that requires sanitization);

degaussing (degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state); or physical destruction (complete physical destruction of PII by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated).

3. Timing. Unless otherwise requested or directed by the President of the Board of Directors or the Association's counsel, files, including PII, should be destroyed as follows:
    a. Physical and Electronic File Destruction
        1. Physical and electronic files that may contain PII, such as ledgers for delinquent owners' accounts, may be destroyed at the earlier of thirty (30) days after the owner sells his or her lot, or three (3) years after the date of the file's creation. The Board of Directors may authorize such destruction, and may delegate the determination of when a file should be destroyed to an officer, its manager, or its legal counsel.

F. Security Breaches

In the event of a security breach occurs that compromises PII or other personal information (as defined in C.R.S. 6-1-716), the Association will follow the procedures and requirements of C.R.S. 6-1-716.

C.D.S. Homeowners Association, Inc., dba
Yosemite Village Homeowners Association,
a Colorado nonprofit corporation

By: Willard Ray Vanvorhes
President

The following Policy Regarding Maintaining, Destruction and Disposal of Personal Identifying Information and Notifications of Security Breaches was adopted by the Board of Directors on the 15th day of January, 2019, effective the 1st day of January, 2019, and is attested to by the Secretary of C.D.S. Homeowners Association, Inc.

Nancy L Morris
Secretary