Eldorado
Neighborhood Second HOA

Safeguarding Personal Information Policy

WHEREAS, Eldorado Neighborhood Second Homeowners Association (the "Association") is a Nevada nonprofit corporation governed by the laws of the State of Nevada, including Nevada Revised Statutes ("NRS") Chapter 116, which governs common Interest communities.

WHEREAS, NRS 116.3102(1) (a) provides that an association may "adopt and amend rules and regulations".

WHEREAS, Article 4 Section 4.2 of the Declaration of Covenants, Conditions and Restrictions and Reservation of Easements for Eldorado Neighborhood Second Homeowners Association (the "Declaration") empowers the Board, acting on behalf of the Association, to conduct, manage and control the affairs and business of the Association and to make such rules and regulations therefor not inconsistent with law, the Articles and the Bylaws.

WHEREAS, NRS 603A.2 1 0 requires data collectors that collect, handle, or disseminate nonpublic personal information to enact reasonable security measures to protect such information from unauthorized access, acquisition, destruction, use, modification or disclosure.

WHEREAS, the Association and/or its managing agent is a "data collector" as defined by NRS 603A.030 being a Nevada business entity or association that for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

WHEREAS, NRS 603A.040 defines "personal information" as follows:

1. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
    a. Social security number.
    b. Driver's license number, driver authorization card number or identification card number.
    c. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

d. Any medical identification number or health insurance identification number.
e. A username, unique identifier, or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

2. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the public from federal, state or local governmental records.

WHEREAS, the Association (including the Board), its agents, and volunteers may acquire nonpublic personal information in conjunction with carrying out the Association's duties and responsibilities in one or more of the following circumstances:

- The Association may proactively request and collect such information in carrying out its responsibilities under the law and Governing Documents such as when the Association requests a social security number to verify eligibility for protection under the Nevada Servicemembers' Civil Relief Act or a copy of a voided check with a bank account number to set up direct debt assessment payments.

- Alternatively, the Association may inadvertently acquire such personal information when it is included as part of other documents. For example, the collection file on an Association-foreclosed unit may include the name and driver's license number of the high bidder or an Owner seeking reimbursement from the Association may submit a copy of an invoice or statement on which a credit card number has been written out.

- Nonpublic personal information may be faxed or emailed to the Association or delivered in hardcopy via the mail. An Owner may hand deliver an original document, such as a driver's license, which is copied for the Association's records using a digital copy machine.

KNOW, THEREFORE, BE IT RESOLVED that the Board of Directors hereby adopts the following Policy for safeguarding personal information:

1. The Association shall take reasonable measures to safeguard this nonpublic personal information by adopting administrative, record storage and data security procedures developed in consultation with appropriate professionals.

2. This policy and related procedures shall be distributed to the Board, the managing agent, and volunteers on an annual basis.

3. The managing agent shall ensure that each person working on the Association's account understands the definition of nonpublic personal information and can identify the most common sources by which the Association receives this information and the steps which must be taken to secure it. On an annual basis, the Community Manager shall provide the Board with a written acknowledgement that this information has been reviewed with the managing agent's employees.

4. Unless the person's duties involve routine review or processing of nonpublic personal information, any person encountering nonpublic personal information in any document in the Association's possession or control shall immediately bring it to the attention of the Community Manager so that it may be properly secured.

5. The Board shall establish reasonable safeguards for storing its nonpublic personal information. Such safeguards may include, but are not limited to:
    a. Use of encryption to ensure the security of electronic transmission of data meeting the standards set forth in NRS 603A.215. Pursuant to NRS 603A.2 l 5(2), a data collector shall not transfer any personal information through an electronic, non- voice transmission other than a facsimile to a person outside of the data collector's secure system unless it uses encryption to ensure the security of the electronic transmission.

    b. Segregation of nonpublic personal information from other generally accessible data. This may include ensuring that personal information is maintained in locked files separate from the general homeowner files; a separate password protected 'filing cabinet" exists within an electronic record storage system for personal information, or access to screens, reports or programs within the management/accounting or access software where such personal information is stored is restricted.

    c. Limitations on the number and types of persons (e.g., Community Manager, Accounting Manager, Board Treasurer) who are authorized to access or process nonpublic personal information in the Association's or its managing agent's possession.

    d. Requirements for the proper disposal of nonpublic personal information.

    e. If the Association or its managing agent accepts credit cards, debit cards or any other cards meeting the definition of "payment card" pursuant to NRS 205.602, compliance with the current version of the Payment Card Industry (PCI) Data Security Standard as set forth in

NRS 603A.215.

6. The Association shall maintain insurance covering a breach of nonpublic personal information.

7. Contracts with agents and vendors, including but not limited to those who may have access to: (1) the Association's computer system through the internet or by servicing data storage devices on site, (2) paper records through a document destruction or a paper to electronic storage conversion contract or (3) contractors who create and store Association records on software such as management/accounting software or gate access control software, shall include provisions addressing the security of nonpublic personal information. Pursuant to NRS 603A.215(2)(b), a data collector shall not move any data storage device containing personal information beyond the logical or physical controls of the data collector, its data storage contractor or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information, unless the data collector uses encryption to ensure the security of the information.

8. In the event the Association discovers an unauthorized acquisition of computerized or hard copy data that materially compromises the security, confidentiality, or integrity of personal information in the Association's records, the Association shall promptly notify the affected person(s) of the breach unless a law enforcement agency determines that the notification would impede a criminal investigation. However, as soon as the law enforcement agency determines that the notification will not compromise the investigation, the Association shall notify the affected person(s). See NRS 603A.220.

9. The Association shall take reasonable measures to ensure the destruction of records containing nonpublic personal information when retention of such information is:
    a. No longer necessary; or
    b. No longer required to be maintained as part of the Association's books and records pursuant to NRS 116.31175(7).

"Reasonable measures" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable. See NRS 603A.200(2)(b).

10. When the Association no longer needs access to nonpublic personal information in its un- redacted form (e.g., when the person to whom the information applies is no longer a resident of the community), the

Association shall redact the information by using commercially available redaction software for scanned or electronic records, securely deleting the un-redacted document, or by manually redacting information retained in hardcopy.

11. Pursuant to NRS 116.31175(7), at the end of 10-year record retention period, the Association shall destroy any outdated nonpublic personal information by:
    a. Shredding any hard copies.
    b. Securely deleting personal information from electronically maintained records.

12. Before selling, donating, exchanging, or decommissioning any data storage device, including but not limited to, computers, cell phones, electronic computer drives, optical computer drives, digital copiers and multi-function printers, the Association shall ensure that all data has been securely deleted from the device. Lost or stolen data storage devices shall be promptly reported to the Community Manager.

On an annual basis, the Board shall cause a review of Association operations to (I) identify what processes, procedures, activities, or services may result in the collection of nonpublic personal information, (2) test that privacy protection procedures are functioning as intended, and (3) revise this policy or its procedures. As new services or technologies are added, the Board shall consider whether such services or technologies will result in the Association collecting nonpublic personal information and how such information will be secured.

If any provision of the Policy is determined to be null and void, all other provisions of the Policy shall remain in full force and effect. This resolution of the Board of Directors has been duly adopted at the January 11, 2024 Executive Board of Directors meeting.

By: _____ _____
President — Lyle E. McKenzie, President — Date

By; _____ _____
Vice President — Date

By: _____ 2/8/2024
Treasurer — Date

By: _____ 1/28/2024
Secretary — Jimmie McKinney, Secretary — Date

By: _____ 2-9-2024
Director — Date

By: ---------- ----------
Director — Date

By: _____ 2-8-2024
Director — Date