Approved by the Board of Directors on September 20, 2022

River Acres WSC
Personally Identifiable Information Policy

Policy Statement

It is the policy of River Acres WSC (RAWS) to protect personally identifiable information (PII) of employees, RAWS members, RAWS customers, contractors, vendors, clients, and board members. The electronic restrictions and safeguards outlined in this policy provide guidance for employees, board members, contractors, vendors, and clients that have access to PII retained by RAWS to ensure compliance with state and federal regulations.

Definitions

PII is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is an employee, board members, contractors, vendors, and clients.

Sensitive PII includes but not limited to Social Security Numbers (SSN), drivers license, phone numbers, address, and account numbers/info. This data requires stricter handling because of the increased risk to an individual if the data is compromised.

Procedures

This section provides guidelines on how to maintain and discard PII. If current procedures fall outside this policy or questions arise, please suggest more efficient procedures for protecting PII to the board of directors. All electronic files that contain Protected PII will reside within a protected information system location. All physical files that contain Protected PII will reside within a locked file cabinet or room when not being actively viewed or modified. Protected PII is not to be downloaded or transferred to personal electronic devices (such as laptops, personal digital assistants, mobile phones, tablets, or removable media). PII will also not be sent through any form of unsecure electronic communication E.g., Online Form, E-mail, or instant messaging systems.

PII will not be available for viewing, copying or removal from the RAWS office by ANYONE without prior authorization by the board of directors.

Incident Reporting

President, Vice President, or Sectary/Treasurer must be informed of a real or suspected disclosure of Protected PII data within 24 hours after discovery. E.g., Misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII.

Audits

Periodic audits of Corporation's owned equipment and physical locations may be performed to ensure that protected PII is stored in approved information systems or locations. The purpose of the audit is to ensure compliance with this policy and to provide information necessary to continuously improve practices.

Enforcement

An employee, board member, contractor or vendor found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation. If it appears to be that an individual, group, or organization is gathering information on an individual, or group of individuals; maybe be reported to the Texas AG and or the local AG.

Records Disposal

For more information on Records Disposal, refer to the Document Retention and Destruction Policy.