ZINI RIVER ESTATE HOME OWNERS' ASSOCIATION ("ZREHOA")

Policy:

Data Security 2022

This is a confidential document not for dissemination or use outside the ZREHOA

POLICY VERSION CONTROL

Information Officers Name	Mrs. Rose Brown
Information Officers Email	estatemanager@zrehoa.co.za
Deputy Information Officers Name	Mrs. Jenny-Lynn Broadhurst
Deputy Information Officers Email	bookkeeper@zrehoa.co.za

The Information officer recommended the adoption of the policy:

DESIGNATION	APROVAL DATE	SIGNATURE
Board of directors	30 August 2022	

Next review date: _____

TABLE OF CONTENTS

PART A: DATA SECURITY FRAMEWORK

1. PURPOSE

1.1. To provide a framework for data security ("data security") at the ZREHOA in order to protect the ZREHOA's data in a manner commensurate to its value as well as ensure accountability in respect of and protection of ZREHOA client data (hereinafter referred to as "data").

1.2. To establish appropriate governance arrangements for the obtaining, protection, management and use of ZREHOA data, the prevention of unauthorised access to or processing of data, the prevention of accidental loss / destruction of data, and the reduction of the risk of potential threats and liability for unauthorised or improper use of data.

1.3. To educate employees and third parties in respect of their obligation and responsibility to protect data and ensure its security.

2. PRINCIPLES

2.1. The ZREHOA is committed to high standards in respect of the protection of its data and views data security as a key strategic priority for the ZREHOA.

2.2. Data security is vital for public and client confidence and necessary for the effective and safe conduct of the ZREHOA's business and the appropriate, lawful and secure management of sensitive and personal data and information.

2.3. Data must be protected in all its forms during all phases of its life cycle from inadvertent compromise or unauthorised or inappropriate access, use, modification, disclosure or disposal. The typical life cycle of data at the ZREHOA is: use of data; transmission of data; storage of data; and disposal of data.

2.4. Data access must be enforced on a "need to know" and "need to have basis".

2.5. The "ZREHOA data environment" to which this policy applies, comprises of:

2.5.1. *Applications* – general or specific software applications or programmes designed for use by employees and clients, supporting business or end-user jobs or functions.

2.5.2. *Systems* – an assembly of computer hardware (workstations, laptops, printers, photocopiers, servers, etc.) and application software for processing, handling, transmitting, receiving and storing data in support of business tasks and processes.

2.5.3. *Networks* – two or more systems connected by a communication medium, including all hardware and elements related to such networks (routers, switches, hubs, bridges, firewalls, etc.) that are used to transport information between systems.

2.6. Persons should as far as possible be granted only such necessary privileges in the ZREHOA data environment as required by them to accomplish their duties, and no more. Accordingly, access to data should be on an authorised, 'need to know' basis to restrict access to only those properly authorised to the extent such is reasonably possible.

2.7. Persons should be accountable for their actions requiring the ZREHOA data environment to be structured as effectively as possible to allow for the identification, authentication and auditing of all user actions within the ZREHOA data environment.

3. SCOPE

3.1. This policy applies to all data in whatever form and medium as such is contained and stored in the ZREHOA environment, other than data which is identified as public by the ZREHOA or would generally be regarded as public in accordance with good industry practice.

3.2. This policy forms part of the conditions of employment of all ZREHOA employees (permanent and temporary) who have access to ZREHOA data, who must abide and comply with its provisions.

3.3. This policy informs the ZREHOA's contractual arrangements with third party vendors, suppliers, service providers and correspondent firms (collectively referred to as "third parties") who have access to ZREHOA data.

3.4. This policy forms part of and is integral to the compliance by the ZREHOA with the Protection of Personal Information Act 4 of 2013 ("POPIA") and must be applied together with the policies and procedures of the ZREHOA in respect of POPIA.

4. BREACH OF POLICY

4.1. Intentional or negligent misuse of data or action/inaction by an employee of the ZREHOA that results in a breach of this policy will result in disciplinary action being taken by the ZREHOA against such employee. Any breach of this policy shall be viewed with severity by management and disciplinary action, including for repeated infringements of this policy, shall reflect the severity of such conduct.

4.2. Any third party that breaches any of the ZREHOA's contractual arrangements with such third party in respect of data privacy and security may, without limiting the ZREHOA's other remedies or ability to claim damages, be seen as constituting grounds for termination of their contracted services.

5. GOVERNANCE

The following governance structures in respect of data security are established by this policy:

5.1. Board of Directors

The ZREHOA Board of Directors has ultimate responsibility for data security within the ZREHOA and is required to ensure the implementation of this policy, its oversight and annual review.

5.2. Information Technology Committee

The ZREHOA's Information Technology Committee assists the Board of Directors in fulfilling its governance responsibilities and oversees the implementation of the policy, risk management, compliance and operational controls in respect of data security.

5.3. Information Officer

5.3.1. The ZREHOA Deputy Information Officer appointed under POPIA, will also be the ZREHOA's designated Information Security Officer (ISO). The ISO can further delegate any of his/her responsibilities to a deputy ISO.

5.3.2. The ISO reports to the Information Technology Committee on the implementation of the policy within ZREHOA, the maintenance of standards required by the policy as well as any reports or incidents relating to data security.

5.3.3. The ISO must facilitate compliance by the various ZREHOA departments with this policy.

5.4. Employees (permanent and temporary)

The role of employees is vital in ensuring that information is held securely by the ZREHOA. All employees must take responsibility for the protection of data that they manage or have access to as part of their day-to-day activities and must ensure that such data is kept secure and is protected against unauthorised or unlawful use, loss or disclosure in accordance with this policy.

6. MONITORING AND REPORTING

Effective monitoring and reporting procedures are required to ensure that data security standards are in place and maintained:

6.1. Annual Data Security Report

The ISO shall annually report to the Board of Directors on the efficiency and effectiveness of the data security measures contained in this policy, risk assessment of potential vulnerabilities and threats, suggested policy changes and budgetary requirements for the implementation of data security measures.

6.2. Incident Monitoring and Reporting

Important to the effectiveness of this policy is the timely reporting of all suspected incidents of misuse, loss of data or any breach of data security in accordance with the ZREHOA's policies on data breach incidents and response.

7. TRAINING

Effective training on data security ensures that a secure data environment at the ZREHOA is maintained:

7.1. General Data Security Training

The ZREHOA will periodically provide training to all ZREHOA employees in respect of data security to ensure that employees are aware of and have an up-to-date knowledge and understanding of the ZREHOA requirements in respect of data security and that a consistent standard prevails throughout the ZREHOA.

7.2. Employee induction

Any new employee commencing employment at the ZREHOA must be made aware of the ZREHOA's data security policy and requirements and that compliance therewith is a condition of their employment with the ZREHOA.

7.3. Specialist training

Where necessary and approved by the Information Technology Committee, additional specialist training in respect of data security may be procured by the ZREHOA from time to time.

8. COMMUNICATION

8.1. This policy shall be made available to all employees on the ZREHOA's [intranet / network / website] and can also be obtained from the office of the ISO.

8.2. Any changes, amendments or revisions of this policy shall be communicated to all employees by means of internal email and an updated version of the policy shall be made available to employees in accordance with paragraph 8.1.

9. AUDITS

The ISO may undertake periodic internal audits of compliance by ZREHOA departments with the provisions of this policy, and where necessary and [with the approval of the Board of Directors][1] procure the assistance of external specialists to assist in conducting audits and implementing remediation measures.

PART B: DATA SECURITY CONTROLS

GOVERNANCE

10. CLIENT PERSONAL INFORMATION

Employees must comply with the ZREHOA's POPIA Policy in respect of any processing of Personal Information (as defined in such POPIA) of clients.

11. CONTRACTS OF EMPLOYMENT

11.1. All employment contracts (permanent or temporary) must contain provisions in respect of data security which should be similar in form to the draft wording provided below:[2]

*"1. **Data Security***

The employee, by his/her signature hereof, acknowledges that -

1.1 he/she has read and understood the ZREHOA Data Security Policy and the related documents mentioned therein, understands that such, and any amendments thereto as communicated to the employee from time to time, forms part of his/her conditions of service, and considers himself/herself bound by its provisions;

1.2 he/she may during the course of his/her employment with the ZREHOA, gain access to or become acquainted with private, confidential and sensitive ZREHOA and client information, and undertakes that for the duration of his/her employment as well as indefinitely after termination thereof, not to in any manner or form, or in any medium, or by any action or inaction, directly or indirectly, utilise, disclose, make public, convert or publish such information or enable access to such information by any third party and to at all times keep such information secret and confidential, unless such

[1] ZREHOA can decide to require such procurement to be subject to board approval to ensure that the ISO does not have an open mandate on such appointments.
[2] This should be included specifically for data security and can be in addition to or incorporated with any other normal restraint of trade clause and non-disclosure / confidentiality provisions as well as POPIA consent provisions.

disclosure is required by law or in the normal course of business and the execution of the employee's duties and with the imposition of similar non-disclosure obligations on the receiving party to the extent allowed by law; and

1.3 he/she may be held personally liable for any damage, claims, costs or expenses incurred by the ZREHOA flowing from a breach of the provisions of this clause on Data Security."

11.2. New employees commencing employment at the ZREHOA must be made aware of the ZREHOA's data security and POPIA policies and procedures relating to data security.

12. BACKGROUND CHECKS

12.1. The ZREHOA shall perform a basic background check in respect of potential new employees, verifying employment history and where appropriate to the employment position of the new employee, also their educational qualifications.

12.2. Where the nature of their employment position requires such[3], the ZREHOA shall also conduct credit and criminal background checks of employees prior to their employment as well as periodically during employment, should this be deemed necessary or a client requirement. [4]

12.3. All results of background checks must be included in the employment file of the employee.

13. THIRD PARTY NON-DISCLOSURE

13.1. When any third party needs to be provided access to data of the ZREHOA, any such access must comply with the POPIA Policy of the ZREHOA and where necessary the appropriate confidentiality undertakings or operator agreements should be in place with that third party that provides a basis of for disclosure, treating of information confidentially, indemnification of the ZREHOA and the return or destruction of data upon completion of the third party's contractual obligations of the ZREHOA.

13.2. All concluded agreements with third parties must be centrally stored by the ZREHOA.

AUTHORISATION

14. PASSWORD AND ACCESS CONTROL

[3] This may be a requirement of key clients such as financial institutions, or specific types of software applications, bookkeepers or accounting personnel, etc.
[4] This could be conducted by specialist service providers that provide background check services to employers. Companies can however decide to conduct complete background checks on all new appointments as a standard policy at the ZREHOA.

14.1. Access to data on ZREHOA systems or networks may only occur with appropriate access control and authentication of the user gaining access.

14.2. Every user provided with access to the ZREHOA systems or networks, must be authorised through appropriate credentials (such as login username) and authenticated through the use of a unique password prior to gaining access to the network and/or systems.

14.3. All passwords and password renewals, reset and reissue must comply with the ZREHOA's policies regarding passwords and user authentication.

15. ADMINISTRATOR ACCESS

15.1. All ZREHOA employee desktop computers, laptops and other systems capable of running applications may not allow Administrator Access to employees, unless approved by the Information Technology Committee.[5]

15.2. Employees may only have applications installed that have been approved by the Information Technology Committee and that are directly related to their work descriptions. Any requests for application installations must be directed to the Information Technology Committee.

16. HARDWARE AND PERIPHERALS[6]

16.1. No external hardware and other peripherals (flash disks, hard drives, memory sticks, USB port and other plug-in devices, FireWire, Bluetooth, Infrared, etc.) capable of accessing and transferring files to and from any ZREHOA system or network, will be allowed access to any employee computer/laptop.

16.2. Only authorised devices as approved by the ZREHOA and recorded in an **External Device Register** in relation to each employee will be allowed to access any employee computer/laptop.

17. CHANGE MANAGEMENT

To ensure the integrity of the ZREHOA data environment it is necessary that all changes to the environment are conducted in accordance with a planned changed management process, which shall include:

17.1. Appropriate amendments to ZREHOA policies (where required);

---

[5] If this is not possible or feasible, then the policy on which software applications is allowed on employee computers, should be clearly communicated with disciplinary steps following for unauthorised installation of software. IT support can assist ZREHOA's with installing validation software that track all applications on employee computers, including versions, patches, licencing, etc.

[6] Companies should identify and implement specific software that will govern the access and use of USB and similar ports within the organisation as well as the ability to use CD/DVD-RW drives for the copying of information.

17.2. Testing of changes prior to ZREHOA-wide implementation; and

17.3. Training of employees in new procedures.

USE OF DATA

18. NOTING OF CONFIDENTIALITY

All confidential ZREHOA and client data should as far as reasonably possible and appropriate be identified as such through appropriate disclaimers, watermarks and confidentiality notation on or in relation to such data.

19. E-MAIL SECURITY

Email security is vital to the ZREHOA and forms an integral part of the ZREHOA's data security environment and the ZREHOA's policies on email security and electronic communication must be applied together with this policy.

TRANSMISSION OF DATA

20. DATA COPYING, TRANSFER AND DISTRIBUTION[7]

20.1. No employee may copy, transfer or distribute any ZREHOA or client data in any manner or form for personal or third party use, with the copying, transfer or distribution of data only authorised where directly related to the employee's job function and necessary for the performance of such function and the recipient of any such data is informed of the non-disclosure requirements in respect of such data, and where appropriate, is subject to non-disclosure restraints.

20.2. No employee will be allowed to utilise any file transfer or file upload application, software, website or device without the approval of the Information Technology Committee. Any such use must be for a specific purpose and must be terminated immediately upon such having been completed.

20.3. When sensitive ZREHOA data is being transported all physical media (hard drives, laptops, files, etc.) should be secured in a lockable boot during transit and should not be left unattended within the vehicle.

20.4. Any employee authorised to take ZREHOA data out of the ZREHOA's offices, must ensure that such data is secured in a manner commensurate with the security of such data as if stored at the ZREHOA's offices.

---

[7] Firms should identify and implement specific software that will govern the access and use of USB and similar ports within the organisation as well as the ability to use CD/DVD-RW drives for the copying of information.

21. REMOTE WORKING FACILITIES

Employees that work remotely, either temporarily or on a more permanent basis, must at all times comply with this policy as well as any policies of the ZREHOA relating to remote working by employees.

STORAGE OF DATA

22. BUSINESS CONTINUITY

The business continuity policies of the ZREHOA form an integral part of the ZREHOA's data security environment and must be applied together with this policy.

23. DATA BACKUPS

The ZREHOA should ensure appropriate backing up of ZREHOA data in accordance with its business continuity policies, to ensure retention and the ability to restore data in the event of a data breach or data loss incident.

24. ENCRYPTION

24.1. All server data backups must be encrypted[8].

24.2. All remote working devices such as laptops, tablets and mobile devices must be encrypted and have user access control activated. No access to any of the ZREHOA's network, servers or systems may be allowed via such devices without such devices having decryption and user access control activated. All users must ensure their absolute compliance with this requirement and ensure that their device security and access is managed on the same basis as their firm login passwords. Any violation of these requirements will result in any device summarily being disallowed to have any form of access.

25. SYSTEM AND NETWORK PROTECTION

To protect the ZREHOA systems and networks from external threats and attacks, the following minimum protective measures must be applied:

25.1. **Anti-virus detection and removal systems** – daily updated anti-virus programme on all systems and networks.

25.2. **Firewall** – firewall on all systems and networks restricting unauthorised remote access and attacks on system and networks.

---

[8] Firms must evaluate to what extent files and live data can also be encrypted and should discuss the entire encryption and security environment in respect of their servers and back-up information with their IT service provider to ensure that back-up procedures comply with good industry practice.

25.3. **Internet access** – employee usage of their computers and internet must be strictly in accordance with the policies of the ZREHOA in connection with computer usage and electronic communications, which forms an integral part of the ZREHOA's data security environment and must be applied together with this policy.

25.4. **Patch management** – all systems and networks should in a timely manner be updated with the latest security patches as and when such become available.

25.5. **Email security** – all email traffic should be monitored for dangerous and malicious software and attacks on the firm via email.

26. INCIDENT MANAGEMENT

Any breach of data security should be dealt with as an Incident in terms of the ZREHOA's data breach and incidents response plan.

27. PHYSICAL SECURITY

27.1. The ZREHOA server rooms must remain locked and secure at all times with server room access only provided by the ISO. All access keys to the server room shall be retained by the ISO in a secure storage safe.

27.2. The ZREHOA file archive must remain locked and secure at all times with file archive access only provided by the ISO. All access keys to the file archive room shall be retained by the ISO in a secure storage safe.

27.3. All access to the ZREHOA server rooms and file archive must be logged in an Access Register maintained by the ISO, logging all access times and dates and the reason for access.

27.4. Public access to the ZREHOA must be via controlled access points. Public access points must be secured outside of formal business hours with access by employees through unique access cards, security notifications and security system passwords for accessing the ZREHOA premises, allowing identification of employee ingress / egress from the premises.

27.5. 24 hour security support, including armed response, must ensure that the ZREHOA perimeter is secured from unauthorised breach and security intrusions.

27.6. All ZREHOA office areas must be locked / secured during periods of absence of employees from such areas, which duplicate access keys retained in a secure storage safe.

27.7. Where possible video surveillance should be in place in respect of server rooms and main building exits.

DISPOSAL OF DATA

28. DATA DISPOSAL

28.1. ZREHOA data (physical and electronic) may be disposed of after [seven][9] years from date of finalisation of the matter, unless a longer period is required by law or agreed to with the client.

28.2. All physical data must be disposed of by shredding and destruction by authorised waste disposal vendors that provide a Certificate of Confidential Disposal. The ZREHOA will provide confidential waste bins that must be used to deposit physical data that must be confidentiality destroyed.[10]

28.3. Electronic systems that contain ZREHOA or employee data (computers, laptops, servers, etc.) that are disposed of or re-assigned, must prior to such disposal or re-assignment have all such data completely removed with a certificate issued by the ZREHOA's information technology service provider certifying such cleansing.

[9] Longer periods may be required in terms of legislation, and Companies should consider this.
[10] Companies can provide locked bins for confidential waste, or these can be procured from service providers that offer secure waste disposal services that place and remove bins and issue certificates for disposal.