Retirebest

Information Security Policy

Retirebest.

INFORMATION TECHNOLOGY SECURITY AND PROTECTION OF PERSONAL INFORMATION POLICY

for

RETIREBEST (PTY) LTD

registration number: 2022/244873/07

1. Introduction

Retirebest is a retirement planning company that uses it digital platform to provides retirement counselling and advice, either directly or in partnership with other vendors.

Retirebest is committed to protecting the privacy of its customers and recognises its legal obligations when it comes to the collection, processing and distribution of personal information.

2. Purpose

The deliberate or accidental disclosure of any personal information has the potential to harm the Retirebest business and customers. This policy is designed to minimise that risk. The purpose of this policy is to:

- Reduce the risk of IT problems.
- Demonstrate how Retirebest safeguards the information of its employees and clients.
- Ensure that employees of Retirebest comply with all the legal and professional obligations.
- Provide direction on how to manage comply with the Protection of Personal Information Act 4 of 2013.
- Regulate how personal information is processed.
- Establish measures to ensure respect for and to promote, enforce and fulfil the rights of Retirebest's clients.

3. Scope

This policy applies to anyone including employees, partners and temporary contractors that have access to or work with the information obtained through Retirebest and/or any Retirebest clients. This policy does not apply to information collected, processed or distributed by third parties that Retirebest does not control.

This policy must be read together with all of Retirebest's company polices.

4. Definitions

AWS	means Amazon Web Services
Consent	means any voluntary, specific and informed expression of agreements
Data Subject	means the person to whom the personal information relates

De-identify means to delete information that

a) identifies the data subject
b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
c) can be linked by a reasonably foreseeable method to other information that identifies the subject

Personal information means any information that could be used to identify a data subject and includes

a) race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, birth
b) education, medical history, financial history, criminal history, employment history
c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to a person (such as postal address)
d) opinions, views, preferences of the data subject and opinions or views of another person about the data subject;
e) correspondence
f) name

Processing as it relates to personal information means any operation or activity, whether or not by automatic means, including:

a) collecting, receipt, recording, organising, collation, storage, updating, modification, retrieval, alteration, consultation or use;
b) dissemination by means of transmission, distribution, or making available in any form;
c) merging, linking, degrading, erasure or destruction

Record means any recorded personal information, regardless of its form or medium that is in Retirebest's possession or under its control

5. Responsibilities

Neil Botha is the director with overall responsibility for this policy and for Retirebest's IT security strategy.

Michael du Toit and Alan Rainnie have day-to-day operational responsibility for implementing this policy

6. Processing Information

We will only process information that is necessary for the specific purpose for which it is collected. We will also limit access to personal data to only those that need it for processing.

We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources appropriately:

- Unclassified. This is information that can be made public without any implications for the company, such as information that is already in the public domain.
- Employee confidential. This includes information such as medical records, pay and so on.
- Company confidential. Such source code, business plans, policies, passwords for critical IT systems, client contact records, accounts etc.
- Client confidential. This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information and customer's personal and credit information.
- Business partner confidential. Such as annuity rates from annuity providers.

We have categorised the information we keep as follows:

Type of information	System involved	Classification level
Marketing material		Unclassified
Employee contracts, medical records, pay records, leave records	G-Suite: Admin: Alan Rainnie	Employee confidential
List of passwords for critical IT systems	○ Firebase ○ Vercel ○ MongoDB Admin: Michael du Toit	Company confidential
Customer personal information	○ User Admin Panel Admin: Alan Rainnie	Client confidential

7. Access Control

In general, administrative privileges to company systems will be restricted to specific, authorised individuals where it is necessary for the proper performance of their duties.

Users are added to specified security groups in the following procedure:

- The user requests or is nominated as a member of security group due to their business duties or requirements.
- User request is validated by Retirebest IT staff.
- User request is validated by Retirebest senior staff (Neil Botha or Alan Rainnie).
- Retirebest IT staff grants user access to security group.
- User is notified.

If users are designated for removal from security groups, the following procedure is followed:

- User removal request is validated by Retirebest IT staff.
- User removal request is validated by Retirebest senior staff.
- Retirebest IT staff removes user access to security group.

8. Reporting

Anyone who has a suspicion that personal information has been accessed or acquired by unauthorised person(s) must immediately notify Retirebest management.

As soon as reasonably possible after becoming aware of a potential compromise, Retirebest will notify:

- the Information Regulator that personal information has possibly fallen into the wrong hands; and
- the data subject in question (provided it is possible to determine their identity) in writing to their last known email address/telephone number.

Notification will include sufficient detail regarding the nature of the compromise including:

- possible consequences;
- the measures Retirebest intends to take/has taken to address the compromise;
- recommended courses of action for the data subject to take to mitigate possible adverse consequences; and
- the identity of the unauthorised person(s) that has accessed the information, if known.

9. Security Software

To protect our data, systems, users and customers we use the following systems:

- We do not have server anti-malware as we are using AWS Lambda, which is a serverless solution
- Google Apps Spam filtering
- Google Apps archiving
- AWS VPC and security groups

Our users do not have external access to our systems via web applications, meaning that we do not require firewalls or Web Application Firewalls (WAFs). All of our systems operate via private subnets with no outside internet access. All communication within these subnets is via Transport Layer Security (TLS), ensuring encryption between services. All data stored is encrypted at rest via AES-256 encryption.

10. Employees joining and leaving

When a new employee joins the company, they will be given Employee Access to Google Suite if necessary for their particular role in the company.

We will provide training to new staff and support for existing staff to implement this policy. This includes:

- An initial introduction to IT security, covering the risks, basic security measures, company policies and where to get help;
- Training on how to use company systems and security software properly; and
- On request, a security health check on their computer, tablet or phone.

When people leave a project or leave the company, we will promptly revoke their access privileges to company systems.

11. Individual responsibilities

Effective security is a team effort requiring the participation and support of every employee, partner and associate. It is your responsibility to know and follow these guidelines. You are personally responsible for the secure handling of personal information that is entrusted to you. You may access, use or share personal information only to the extent it is authorised and necessary for the proper performance of your duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to Alan Rainnie.

12. Protect your own device

It is also your responsibility to use your devices (computer, phone, tablet etc.) in a secure way. However, we will provide training and support to enable you to do so (see below). At a minimum:

- Remove software that you do not use or need from your computer.
- Update your operating system and applications regularly.
- Keep your computer firewall switched on.
- Make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date.
- Store files in official company storage locations so that it is backed up properly and available in an emergency.
- Switch on whole disk encryption.
- Understand the privacy and security settings on your phone and social media accounts.
- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers.
- Don’t use an administrator account on your computer for everyday use

- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in.

13. Password Guidelines

- Change default passwords and PINs on computers, phones and all network devices
- Install password management software
- Don’t share your password with other people or disclose it to anyone else
- Don’t write down PINs and passwords next to computers and phones
- Use strong passwords
- Change your passwords regularly
- Don’t use the same password for multiple critical systems

14. Security Risk

While technology can prevent many security incidents, your actions and habits are also important. With this in mind:

- Understand IT security and keep yourself informed.
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender.
- Never disclose personal information, including employee, client or company personal information to outsiders. Fraudsters and hackers can be extremely persuasive and manipulative.
- Be wary of fake websites and phishing emails. Never click on links in emails or social media. Never disclose passwords and other personal information unless you are sure you are on a legitimate website.
- Use social media, including personal blogs, in a professional and responsible way, without violating company policies or disclosing personal information.
- Take particular care of your computer and mobile devices when you are away from home or out of the office.
- If you leave the company, you must return any company property, transfer any company work-related files back to the company and delete all personal information from your systems as soon as is practicable.
- Where personal information is stored on paper, it must be kept in a secure place where unauthorised people cannot see it and shredded when no longer required.

15. Protection of Work-Related Information

Always save work-related items to the designated folders on the local drive as directed by a senior Retirebest staff member. This must be done at the beginning and end of every work day.

The following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

- Anything that contradicts our equality and diversity policy, including harassment.
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of personal information at any time.