QUANTUM WEALTH MANAGEMENT
YOUR SUCCESS | YOUR FREEDOM | YOUR FUTURE

QUANTUM FUND MANAGERS
YOUR SUCCESS | YOUR FREEDOM | YOUR FUTURE

**Quantum Wealth Management (Pty) Ltd**
**Registration number 2001/020621/07**
**FSP No: 862 Category I and II**
**("the Company")**

**Quantum Fund Managers (Pty) Ltd**
**Registration number 2013/208134/07**
**FSP46340 Category II**
**("the Company")**

# Cyber Security Policy ("the Policy")

Walker Creek Office Park Building | Office Co. | 2nd Floor | 90 Florence Ribeiro Avenue | Nieuw Muckleneuk | Pretoria
PostNet Suite #402 | Private Bag X06 | Waterkloof | 0145
**Tel** +27 12 346 0084 | **Fax** +27 86 681 3489 | **Email** info@quantumwealth.co.za | **Web** www.quantumam.co.za

## 1. Policy approval and information

| | |
|---|---|
| Policy owner | Board of directors |
| Policy type | Compliance |
| Policy drafter | Dominique Kielblock |
| Policy reviewer | FC Greeff |
| Policy creation date (1st version) | June 2021 |
| Policy review date (this version) | October 2023 |
| Approver's signature | |
| Approved by (this version) | Stefan Greeff |
| Adopted by (this version) | Board of directors |
| Approval date (this version) | |
| Approval date (1st version) | June 2021 |
| Version number | V01.01 |

Summary of policy history

| Version number | Drafted/adapted/reviewed by | Creation/review date | Approved by | Approval date |
|---|---|---|---|---|
| V01.01 | Dominique Kielblock | FC Greeff | FC Greeff | June 2021 |
| V01.02 | Dominique Kielblock | N/A | N/A | N/A |

## 2. Scope

This policy applies to all our employees, contractors, volunteers, remote workers and anyone who has permanent or temporary access to our electronic systems, software and/or hardware.

The policy addresses the protection of electronic records, especially those of a confidential or private nature.

The Information Officer will be responsible for ensuring implementation of the procedures described in this policy.

This policy should be read together with Quantum's Privacy Policy, Record Retention Policy and the information technology disaster recovery section of the Business Continuity Policy.

## 3. Purpose

The purpose of this policy is to provide guidelines for the protection of data, data security and safeguarding our technology infrastructure. It outlines protocols that govern cyber security measures and define the rules for company and personal use.

## 4. Policy

Quantum takes data security seriously and we are committed to implementing cyber security measures aimed at ensuring the confidentiality, integrity and availability of data.

## 5. Procedures

### 5.1. Own devices and company devices under your control

Using personal digital devices to access company emails or accounts introduces a data security risk.

The following is required:

- Keep all devices password protected;
- Use and regularly upgrade comprehensive antivirus software;
- Never leave devices exposed or unattended;

- Install security updates of browsers and systems monthly or as soon as updates are available;
- Login to company accounts and systems through secure and private networks only; and
- Do not lend own devices to others.

Users must avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

**5.2. Keep emails safe**

Emails often host scams and malicious software. To avoid virus infection or data theft, you must:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing.");
- Be suspicious of clickbait titles (e.g., offering prizes, advice.);
- Check email and names of people messages are received from to ensure they are legitimate; and
- Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If you are not sure that an email received is safe, refer it to Dominique Kielblock who will investigate the matter with the IT specialists.

**5.3. Manage passwords properly**

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, we advise you to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays.);

- Remember passwords instead of recording them. If you need to write down/save a password, keep the paper or digital document confidential and destroy it when it is not required anymore and never keep a written down password with your device;
- Exchange credentials only when absolutely necessary. When exchanging them in-person is not possible, use phone instead of email, and only if you personally recognize the person you are talking to; and
- Change passwords at least every two months.

**5.4. Transfer data securely**

Transferring data introduces security risk. We will:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless absolutely necessary;
- Share confidential data over the company network / system and not over public Wi-Fi or private connection; and
- Ensure that the recipients of the data are properly authorized people or organizations that have adequate security policies.

**5.5. Additional measures**

To reduce the likelihood of security breaches, we also instruct you to:

- Turn off your screens and lock your devices when leaving your desk;
- Report stolen or damaged equipment as soon as possible to Dominique Kielblock, the Chief Operating Officer and Information Officer;
- Change all account passwords at once when a device is stolen;
- Report a perceived threat or possible security weakness in company systems;
- Refrain from downloading suspicious, unauthorized, or illegal software on company equipment; and

- Avoid accessing suspicious websites.

Our IT Specialists:

- Have implanted anti-malware software and access authentication systems;
- Will inform employees regularly about new scam emails or viruses and ways to combat them;
- Will investigate security breaches thoroughly; and
- Follow this policy's provisions as all employees must do.

Physical access to local servers on the premises is restricted, kept behind a security gate, only admin, the compliance function and directors have access thereto.

**5.6. Remote employees**

Remote employees accessing our company's accounts and systems are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

**5.7. Termination of employment**

The employee / contractor's supervisor must confirm to the Information Officer that the employee / contractor's access to any electronic records of Quantum has been terminated (these include, without limitation, access to Quantum's computer systems, emails, and third-party provider login details).

After returning electronic records to Quantum, the employee / contractor is obliged to delete all (without exception) any of Quantum's electronic records and data kept on personal devices.

**5.8. Back-ups of electronic records**

Data kept on internal systems and stored on local servers are backed manually on a weekly basis as well as automatically.

**5.9. External service providers**

We have performed a reference check on external providers and specifically information technology providers and concluded formal agreements with such providers to govern information security related responsibilities.

## 6. Consequences of Non-Adherence

Action that leads or may lead to a security breach will be viewed in a serious light and Quantum will take disciplinary action or consider terminating agreements with the relevant contractor, employee or provider as the case may be.

## 7. Training and Awareness

All staff will receive a copy of this policy.

## 8. Review

This document will be reviewed at least annually to ensure it remains relevant, but also as and when required, when for example new regulations are published.