

Passwords & Security

1. BANKING & FINANCIAL

5

- ☐ Primary bank(s) - online banking username(s) & 2FA method
- ☐ Foreign investments
- ☐ Investment platforms (unit trusts, stockbroker)
- ☐ Retirement funds / pension portals / provident fund
- ☐ Mortgage / home loan portals
- ☐ Mobile banking app PINs (separate from phone lock)
- ☐ ATM / debit card PINs

2. TAX, BUSINESS & PROFESSIONAL

- ☐ SARS eFiling account (personal) - username / branch / 2FA / recovery
- ☐ SARS eFiling (business) - username / branch / 2FA / recovery
- ☐ Business banking
- ☐ Accounting software (Xero, Sage, QuickBooks)
- ☐ Company email / domain registrar / web hosting
- ☐ Payroll systems

- ☐ Primary bank(s) - online banking username(s) & 2FA method
- ☐ Professional body logins (law society, conveyancer portals)

3. E-MAIL & COMMUNICATION

- ☐ Primary personal email - username / recovery email / 2FA
- ☐ Work / business email(s)
- ☐ Secondary / recovery emails
- ☐ Email app passwords (Outlook / Apple Mail)

4. DEVICES & HOME ACCESS

- ☐ Primary phone (iCloud / Apple ID / Google Account) - password / passcode
- ☐ Secondary phone / old phones / SIM PINs
- ☐ Laptop(s) - admin account / disk encryption password
- ☐ Desktop / workstations
- ☐ Tablet(s)
- ☐ Home Wi-Fi SSID & admin password
- ☐ Router admin password

- ☐ Smart home hub (smart locks, thermostat, alarm)
- ☐ TV / streaming device logins (Netflix, DStv Now, Showmax)
- ☐ Printer admin & Wi-Fi details
- ☐ Bluetooth device PINs (cars, speakers)

5. SOCIAL MEDIA & MESSAGING

- ☐ Facebook (personal / business pages / ad accounts)
- ☐ Instagram (personal / business)
- ☐ WhatsApp (main, business)
- ☐ X / Twitter / Threads / LinkedIn / TikTok
- ☐ Telegram / Signal
- ☐ YouTube / channel monetisation
- ☐ Admin access for groups / pages (who else has access?)

6. SUBSCRIPTIONS & RETAIL

- ☐ Utilities portals (municipal accounts, electricity, water)
- ☐ Insurance portals (home, vehicle, life)
- ☐ Medical aid online portal

- ☐ Domain & hosting providers (domain expiry dates)
- ☐ Amazon / Takealot / Shein / Temu / local online stores
- ☐ Magazine / newspaper subscriptions
- ☐ Gym / club memberships
- ☐ Streaming subscriptions (Spotify, Apple Music)

7. HEALTH & MEDICAL

- ☐ Medical aid / insurance logins
- ☐ Hospital / specialist patient portals
- ☐ Pharmacy / repeat medication portals
- ☐ Passwords for devices storing health info (apps)

8. LEGAL & ESTATE

- ☐ Digital safe instructions (who has key / password)
- ☐ Safe / safe deposit box location & key / code

9. CRYPTOCURRENCES & DIGITAL ASSETS

- ☐ Crypto exchange accounts (Luno) – username, 2FA
- ☐ Passwords for any blockchain keys (explicit place of storage)
- ☐ Crypto wallet login details

10. RECOVERY & SECURITY

- ☐ Password manager account (e.g. 1Password, Bitwarden) - master password & emergency contact access)
- ☐ Recovery codes for 2FA apps (Google Authenticator backup / printed codes)
- ☐ List of trusted devices (which phones / tablets have 2FA app)
- ☐ Backup email & phone numbers for account recovery
- ☐ Security questions & answers (and where stored)
- ☐ Biometric lock info and alternative passcodes

11. WORK & COLLABORATION TOOLS

- ☐ Microsoft 365 / Office 365 - admin & user accounts
- ☐ Google Workspace - admin & user accounts
- ☐ Teams / Zoom
- ☐ File sharing (Dropbox, Google Drive, OneDrive)
- ☐ Passwords for shared folders & folder owners

12. EDUCATION & CHILDREN

- ☐ School portals / parent portals
- ☐ University / learning platforms (student portals)
- ☐ Extra-murals / tuition online accounts

13. TRAVEL & TRANSPORT

- ☐ Airline accounts / frequent flyer numbers
- ☐ e-toll / vehicle licensing portals
- ☐ Accommodation booking portals (Airbnb, Booking.com)

14. PHOTOS, MEDIA & PERSONAL FILES

- ☐ Cloud photo services (iCloud, Google Photos)
- ☐ Shared family accounts / albums
- ☐ Backup drives (where encrypted & passphrase)
- ☐ Media library passwords

THE FOLLOWING INSTRUCTIONS MUST BE
KEPT WITH A TRUSTED PERSON IN A
SECURE PLACE AND NOT IN YOUR FILE

THESE INSTRUCTIONS MUST BE KEPT WITH A TRUSTED PERSON IN A SECURE PLACE AND NOT IN YOUR FILE

Instructions in event of death or incapacity

Please contact:

Name: _____

Contact number: _____

Email: _____

Secondary contact number: _____

He / She is in possession of:

- Clear statement who may access the password manager, and how (master password / emergency access)
- Location of physical copies (sealed envelope in safe) – including exact safe location and who has the key
- Location of digital copies (encrypted file path, cloud location, access instructions)
- Preferred method to notify executor (phone, email, lawyer)
- List of high-priority accounts to be accessed first (banking, utilities, will)
- Special instructions for social media & email (e.g. memorialise account, close business pages)