Easy Crypto SA (Pty) Ltd t/a EasyCrypto
Registration number 2018/351198/07
("the Company")

Information security and privacy policy ("the Policy")

1. Policy approval and information

Policy owner	Board of directors
Policy type	Information security
Policy drafter	Gigi Vorlaufer
Policy reviewer	
Policy creation date (1st version)	June 2021
Policy review date (this version)	June 2021
Approver's signature	
Approved by (this version)	
Adopted by (this version)	Board of directors
Approval date (this version)	
Approval date (1st version)	
Version number	V01.02

Summary of policy history

Version number	Drafted/adapted/reviewed by	Creation/review date	Approved by	Approval date
V01.01	Gigi Vorlaufer (generic draft)	June 2021	N/A	N/A
V01.02	Gigi Vorlaufer (adapted for Company)	June 2021		

2. Purpose and scope

The Information security and privacy policy is prescribed in terms of the Electronic Communications and Transactions Act 25 of 2002 (the ECTA), as amended, or substituted, from time to time. A supplier that offers goods, or services, for sale, for hire, or for exchange, by way of an electronic transaction, must make specific information available to consumers, on the website where the goods, or services, are offered. Amongst several other things, the website must include the security procedures and privacy policy of the supplier, in respect of payment, payment information, and personal information. The website must also include the return, exchange, and refund policy of the supplier.

The Company is a crypto assets service provider (CASP). It has voluntarily applied the obligations applicable to accountable institutions (AIs), in terms of the Financial Intelligence Centre Act 38 of 2001 (the FICA), through the Financial Sector Regulation Act 9 of 2017 (the FSRA), because it is a CASP, and it wants to proactively implement a risk-based approach to mitigate the risk of the Company being used for money laundering and/or terrorist financing. It is an employer, and must adhere to the related employment, labour, health and safety, and taxation, legislation. The Company may provide these services to clients, by providing for clients to transact electronically, via the website, and/or mobile application. A "**transaction**" is either of a commercial, or non-commercial, nature, and includes providing information electronically, and providing e-government services. **The Company is a "data controller", because it electronically requests, collects, collates, processes, or stores, personal information from, or in respect of, a data subject**. The ECTA applies to personal information that was collected through electronic transactions.

This Policy must be read together with the Protection of personal information policy, in terms of the Protection of Personal Information Act 4 of 2013 (the POPIA), the Retention of documents policy, and the manual, in terms of the Promotion of Access to Information Act 2 of 2000 (the PAIA).

The Company's information systems, and computing assets (either leased, or owned), including, but not limited to, computers, data, computer networks, hardware, software, mobile devices, printers, and any other media, used to store, or process, information, are the property of the Company, and are valuable corporate assets.

The purpose of this Policy is to:

- determine the procedures, and minimum standards, which are necessary to ensure the protection, and safeguarding, of the confidentiality, integrity, and availability, of business information, and information processing facilities
- specify the principles for electronically collecting personal information
- determine the procedures for electronic communication
- specify the security safeguards required in terms of Condition 7 of the POPIA
- enable the identifying of information related risks, report unauthorised information access, leakages, or attempts to obtain information, through unauthorised ways
- ensure that electronic transactions conform to the highest international standards
- develop a safe, secure, and effective, environment for clients to use electronic transactions
- specify certain obligations, and prohibitions, about cybercrime.

This Policy is applicable to all employees, regardless of whether they are permanent, temporary, or contractors, third parties, external contractors, consultants, product suppliers, and services suppliers, as may be applicable, and for ease of reference, are collectively referred to as "applicable people". It applies to all the Company's information systems, including systems that are leased, maintained and/or supported by third parties, on behalf of the Company, ad information system services.

2.1. Legislative framework

The reference to legislation, subordinate legislation, and supervision documents, includes amendments made from time to time.

- Electronic Communications and Transactions Act 25 of 2002 (the ECTA)
- Protection of Personal Information Act 4 of 2013 (the POPIA)
- Promotion of Access to Information Act 2 of 2000 (the PAIA)
- Consumer Protection Act 68 of 2008 (the CPA)
- Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (the RICA)
- Cybercrimes Act 19 of 2020 (commencement date is still to be proclaimed).

2.2. Data ownership, protection, security, and use

2.2.1. **"Information system"** is a system for generating, sending, receiving, storing, displaying, or otherwise processing, data messages, and includes the Internet.

2.2.2. **"information system services"** includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission, or routing, of data messages between, or among, points specified by a user, and the processing, and storage, of data, at the individual request of the recipient of the service.

2.2.3. The Company's information systems, data, and computer assets, are the property of the Company, and are deemed to be valuable corporate assets.

2.2.4. Applicable people are responsible for the corporate resources entrusted to them.

2.2.5. Applicable people must exercise care, and due diligence, to ensure the integrity, and security, of corporate resources.

2.2.6. Access to company information, and information systems, must be in accordance with the applicable person's role, and responsibilities.

2.2.7. Company information must be protected from intentional, and negligent, damage.

2.2.8. The Company will only intercept communication on its website and/or mobile application, in accordance with the RICA.

2.2.9. Applicable people may not execute network monitoring and/or interception, unless these activities are in accordance with their roles, and responsibilities.

2.2.10. Management reserves the right to intercept and/or monitor electronic communications for internal policy compliance, suspected criminal activity, lack of employee productivity, and other systems management reasons, in accordance with relevant processes.

2.2.11. **"electronic communication"** is a communication by means of data messages.

2.2.12. **"data message"** is data generated, sent, received, or stored, by electronic means, and includes voice, where the voice is used in an automated transaction, and a stored record.

2.2.13. **It is a criminal offence, in terms of the Cybercrimes Act, to disclose a data message, via an electronic communications service,**

- **causing damage to property belonging to, or violence against, a person, or a group of persons (regardless of whether, or not, the disclosure is unlawful, and intentional)**
- **which threatens a person with damage to property belonging to that person, or a related person, or violence against that person, or a related person (if the disclosure is unlawful, and intentional)**
- **which threatens a group of persons, or a person forming part of, or associated with, that group of persons, with damage to property belonging to that group of persons, or a person forming part of, or associated with, that group of persons, or violence against the group of persons, or a person forming part of, or associated with, that group of persons,**

  and a reasonable person, in possession of the information, with due regard to all the circumstances, would perceive the data message, either by itself, or in conjunction with another data message, or other information, as a threat of damage to property, or violence to a person, or category of persons, respectively (if the disclosure is unlawful, and intentional)
- **of an intimate image of a person, without the consent of that person (if the disclosure is unlawful, and intentional).**

2.2.14. **The Company, as a financial institution, MUST REPORT to the South African Police Service (SAPS), without delay, and preferably not later than 72 hours after becoming aware of the offence, that its electronic communications service, or electronic communications network, has been involved in the commission of cybercrime offences, which offences include:**

- **unlawful access**
- **unlawful interception of data**
- **unlawful acts in respect of software, or hardware, tool**
- **unlawful interference with data, or computer program**
- **unlawful interference with computer data storage medium, or computer system**
- **unlawful acquisition, possession, provision, receipt, or use, of password, access code, or similar data, or device**
- **cyber fraud**
- **cyber forgery, and uttering**
- **cyber extortion**
- **aggravated offences**
- **theft of incorporeal property**

2.2.15. The Company has established appropriate, reasonable, technical, and operational, measures to protect personal information, in accordance with the requirements of the POPIA. **Refer to the Protection of personal information policy.**

2.2.16. The measures have been established to prevent the damage, loss, or destruction, of personal information, and the unauthorised access to personal information.

2.3. Electronically collecting personal information

2.3.1. The Company, as a **data controller**:

- **MUST HAVE** the **express written permission** of the data subject, for collecting, collating, processing, or disclosing, any personal information about the data subject, **UNLESS** it is permitted, or required, to do so, by law.
- **MAY NOT** electronically request, collect, collate, process, or store, personal information about a data subject, which is not necessary for the lawful purpose for which the personal information is required.
- **MUST** disclose, in writing, to the data subject, the specific purpose for which personal information is being requested, collected, collated, processed, or stored.
- **MAY NOT** use the personal information for any other purpose than the disclosed purpose, without the express written permission of the data subject, **UNLESS** it is permitted, or required, to do so, by law.
- **MUST**, for as long as the personal information is used, and **for at least one year** thereafter, **keep a record** of the personal information, and the specific purpose for which the personal information was collected.
- **MAY NOT** disclose personal information held by it, to a third party, **UNLESS** required, or permitted, by law, or specifically authorised to do so, **in writing**, by the data subject.
- **MUST**, for as long as the personal information is used, and **for at least one year** thereafter, **keep a record of the third party**, to whom the personal information was disclosed, and of the **date** on which, and the **purpose** for which, it was disclosed.
- **MUST** delete, or destroy, all personal information that has become obsolete.

2.3.2. The Company, as a party controlling personal information, **MAY USE** that personal information to compile profiles, for statistical purposes, and may freely trade with the profiles, and statistical data, **IF** the profiles, or statistical data, **CANNOT BE LINKED** to a specific data subject, by a third party.

2.3.3. **Refer to the Protection of personal information policy.**

2.4. Privacy

2.4.1. When designing, and developing, business processes, and systems, the Company must consider, and incorporate, privacy principles, such as:

- **Protection**: ensuring that it has taken reasonable steps to protect information from misuse, and keeping the information secure
- **Minimality**: only collecting the minimum information necessary, to achieve a specified purpose
- **Transparency**: not using the information collected for any other purpose, unless permitted by the data subject, or authorised, or mandated, by law
- **Accuracy**: maintaining the information collected in an accurate, timely, and complete, way, to ensure that the interests of the data subjects are protected
- **Security**: implementing suitable physical, and information, security measures, to ensure that collecting, using, and maintaining, personal information, is properly safeguarded.

2.5. Secure environment

2.5.1. The Company must implement, and maintain, security controls to information assets, which are commensurate with the magnitude of harm that would result from the loss of, misuse of, modification of, inability to access, or unauthorised access to, information in a system.

2.6. Information asset priority

2.6.1. The Company will, according to determined criteria, prioritise information assets, based on their business critical nature, the sensitivity of the information, and whether the information needs additional protection, or special handling.

- Highly sensitive information systems, information processing, or services, which require additional protection, must be securely isolated, including on mobile, and portable, devices.

2.6.2. The Company will ensure that information assets have "nominated owners", to ensure the accountability of systems, equipment, and information.

2.6.3. The Company will implement, and maintain, identification, and authentication, measures, to access information systems.

2.6.4. The Company has established documented procedures to securely, manage, and operate, information processing facilities, to prohibit unauthorised disclosure, duplication, modification, destruction, loss, misuse, or theft, of information, and to prohibit unauthorised access to information. These security procedures include both hardware, and software, methods.

2.6.5. The Company has established a business continuity and recovery policy and plan:

- **Business continuity:** To cater for exceptional risks which, even though they are unlikely, would have catastrophic consequences, for the business of the Company, including succession planning, the death of a key person, crisis events that threaten to shut down business operations, or any other financial situation, or unexpected event, which threatens to destroy the business of the Company.
- **Disaster recovery:** To recover, and protect, business operations, being every business subsystem, and operation, if a disaster occurs, being the abrupt disruption of all, or part, of the Company's business operations.
- **Financial recovery:** To restore the Company's financial situation after a significant deterioration.
- **Resolution:** To have a strategy for the rapid, and orderly, resolution of the Company's business, if a failure occurs.

2.6.6. **Refer to the Business continuity and recovery policy and plan.**

2.7. Access, passwords and usernames

2.7.1. Applicable people will be held accountable, and responsible, for activities performed with their usernames for information systems.

2.7.2. Applicable people are prohibited from sharing their usernames and/or passwords for information systems, with any other person.

- Using another person's username and/or password is prohibited.
- When applicable, management will approve the relevant rights, and privileges.

2.7.3. Applicable people must change their passwords for information systems regularly, and when their passwords have been disclosed to other people, or when a system compromise is suspected.

- Where possible:
  - passwords should be set to expire every 30 days
  - passwords should be stored in an encrypted way
  - accounts should be locked after 5 failed incorrect password attempts.

2.7.4. Using generic usernames is prohibited, unless specifically required by the system, and if approved by management.

2.7.5. Usernames may not be re-used for other information system users.

2.7.6. Management reserves the right to intercept and/or monitor the access by applicable people, and third parties.

- Audit logs, which record exceptions, and security related events, will be kept, and monitored.
- Where information systems have been compromised, due to unauthorised access, a root cause analysis must be performed, without delay, to assess the situation.
    - Depending on the situation, the necessary security measures must be rectified and/or enhanced.
    - The required reporting to regulators, and data subjects, must take place, according to the legislative requirements. **Refer to the protection of personal information policy, for reporting security compromises**. **Refer to the relevant section of this Policy, for reporting cybercrime (the reporting method has not been published).**

2.7.7. Applicable people may access the Company's information systems remotely, if management has granted general, or specific, approval.

- Management approves VPN access to its information systems, which should be reviewed regularly, as may be applicable.
- Generally, VPN access is only granted from Company issued devices. However, management may approve access from other devices, as may be applicable.
- The Company reserves the right to provide employees with a mobile data facility, from a service provider of its choice, with data, and network, restrictions, as deemed appropriate.
- Management reserves the right to monitor the use, and take disciplinary action, if deemed necessary.

2.7.8. The relevant IT technicians should regularly monitor for inactive information system accounts, and provide management with a list of the inactive accounts.

- Where applicable, management will authorise the suspending, or revoking, of access to the relevant information system.

2.7.9. When an applicable person's employment, or contract, is terminated, or where the person's roles, and responsibilities, have changed, the relevant IT technicians must be informed about the access that must be revoked, changed, or granted, as may be applicable, effective from a specified date.

2.7.10. Third parties may only be given access to the Company's information systems, if approved by management.

- Before granting access to a third party, management must assess the risks to the business information, information systems, and information processing facilities, and must restrict the access, accordingly.
- Management must regularly re-assess the risks, and the associated access.

2.7.11. Appropriate, written service level, and confidentiality, agreements, must be established with each third party, to whom access has been granted.

2.7.12. Third parties, to whom access has been granted, must not share their usernames, and passwords, with anyone.

2.7.13. The access, username, and password, requirements, and restrictions, are applicable to third parties, who have been granted access.

2.7.14. Third parties, who no longer require access, must notify their contact person at the Company, accordingly, so that the contact person can arrange for the access to be removed.

2.8. Security of information on devices

2.8.1. The Company MUST facilitate the safe processing, and storage of, "**business information"**, which is information that is confidential, personal, or proprietary, to the Company, its employees, or its clients, and which is not aimed at, or intended for, general disclosure to third parties, or the public.

2.8.2. Laptops, and desktops, used by employees, must be issued to them by the Company, for business purposes, to process business information. The laptops, and desktops, should be issued by the Information Technology (IT) department, and should include the base installation, including the minimum security software.

2.8.3. To assist in protecting against unauthorised disclosure, duplication, modification, destruction, loss, misuse, or theft, of information, and to prohibit unauthorised access to information, using external storage devices is not permitted, unless authorised by management.

- External storage devices that have been authorised by management, must preferably use encryption and/or password protection.
- Alternatives, such as Sharepoint, or Microsoft Teams, should be used to move, or share, electronic files.

2.8.4. Employees must report lost, or stolen, laptops, desktops, or external storage devices, to management, as soon as possible after the event, but no later than one week after the event.

- If the employee is unable to make the report, the report should be made by the employee's next-of-kin, to the employee's line manager.
- The theft of Company issued mobile, or portable, devices must also be reported to the SAPS.

2.8.5. Applicable people must take reasonable care to protect their devices from loss, theft, and damage.

2.8.6. If an employee wants to access the Company's IT infrastructure via a smart device, such as a mobile phone, or tablet, they must obtain management authorisation.

- On the smart device, the IT infrastructure must only be accessed using Microsoft Office 365.
- Gaining access to the smart device should be protected using the relevant smart device security settings.
- Management reserves the right to conduct, or request someone to conduct, on their behalf, spot-checks, and audits, of smart devices, to determine the level of compliance with the Policy.

2.8.7. Applicable people, and third parties (to whom access has been granted), must have updated internet security software installed on their devices, which software includes anti-virus protection, advanced threat defence, online threat prevention, vulnerability protection, ransomware remediation, anti-spam protection, firewall protection.

- Employees must immediately report to IT, if they suspect that their internet security software is missing, or faulty.
- Employees must not interfere with, or uninstall, the internet security software installed by the Company.

2.8.8. Employees must not install unlicensed software, privately owned software, or electronic media, on Company issued devices.

2.8.9. Only authorised people may work on a Company issued laptop, or desktop.

2.8.10. Company issued mobile, or portable, devices, may not be lent to another person, without obtaining prior, written, approval.

2.8.11. Employees should not electronically "share" folders, or files, without obtaining prior authorisation.

2.8.12. Employees, other than authorised IT technicians, may not open the casings of Company issued devices.

2.8.13. When employees use their laptops at the Company offices, they should be secured to the desk with a laptop security cable.

2.8.14. Applicable people, and third parties (to whom access has been granted), should take extra care to ensure that strangers are not trying to gather information from their mobile, or portable, devices, when working in public places.

2.8.15. Applicable people, and third parties (to whom access has been granted), who are working in public places, must take extra care to preferably connect to secure Wi-Fi hot spots, and public networks.

- If they do not trust the security of the Wi-Fi hot spot, or public network, they should rather use their mobile device as a personal hotspot.
- They must ensure that the internet security software is functioning, and is updated.

2.8.16. Applicable people, and third parties (to whom access has been granted), who are travelling, must ensure that their mobile, and portable devices, are not left unattended.

2.9. Acceptable use

2.9.1. Applicable people must comply with the Company's policies, and procedures, when using business information, information systems, and information processing facilities.

2.9.2. An applicable person is deemed to have gained authorised access to information systems, when they have entered their unique username, and password, and any required additional authentication methods.

- By default, the applicable person agrees to comply with this Policy, when gaining access to information systems.

2.9.3. Access to information systems is controlled, and restricted, according to a person's seniority, roles, and responsibilities.

- Authorising access to information systems is at the discretion of management.

2.9.4. Applicable people using electronic communication, and information systems, is intended for business purposes. Therefore, personal use must not:

- interfere with normal business activities
- involve solicitation
- be associated with an outside business activity that is deemed to be a conflict of interest
- have any adverse effect on the Company, its associates, its employees, or its clients
- expose the Company, its associates, its employees, or its clients, to reputational risks, or risks of direct, or indirect, losses, regardless of the nature of the losses.

2.9.5. Applicable people must lock their laptops, or desktops, using the "Ctrl", "Alt" and "Delete" keys, or using the "Windows logo" key and the "L" key, when they are not using it.

- Alternatively, they must set the screen to auto-lock after a maximum of 1 minute.

2.9.6. Applicable people must not click on, open, create, send, distribute, or forward, unsolicited messages, such as chain email, hoaxes, unverified virus warnings, using the Company's information systems.

2.9.7. Applicable people must not access, or attempt to access, Company communications that are not intended for them, and they must not create messages, so that it appears as though the sender is another person.

2.9.8. Applicable people must not send messages containing classified information (confidential, personal, or restricted, information), unless they have taken appropriate measures to protect the information, such as encryption, or password protection.

2.9.9. It is prohibited for applicable people to violate the rights of another natural person, or legal person, protected by copyright, trade secret, patent, or other intellectual property, or similar laws, or regulations, including, but not limited to, by installing, or distributing, "pirated", or other software products, which are not appropriately licensed for use by the Company.

2.9.10. Applicable people must not use their Company related email addresses, usernames, or passwords, for their own personal purposes.

2.9.11. Applicable people must not save personal files on the Company's network drives, or information devices.

2.9.12. Applicable people must not advertise, present, promote, solicit, or otherwise make statements about, the Company, unless prior approval has been provided by management.

- This type of communication must be processed according to the Company's advertising, and marketing, procedures.
- The Company will assign "business owners" to manage its social media accounts.

2.9.13. If applicable people save files containing classified information (confidential, personal, or restricted, information), directly on their devices, they must ensure that they have taken appropriate measures to protect the information, such as encryption, or password protection.

2.9.14. Employees should store business information on the relevant, designated, network drives.

2.9.15. Applicable people are prohibited from viewing, storing, or sending, material containing intimate images, discriminatory, abusive, illegal, or contentious, in nature, using the Company's information processing facilities. **To clarify, this includes the disclosure of data messages deemed to be a criminal offence, in terms of the Cybercrimes Act.**

- This type of material must be deleted immediately, and appropriate steps must be taken, to prevent subsequent penetration of the Company's information processing facilities.

2.9.16. In terms of the employment contracts and/or confidentiality agreements, signed by applicable people (as may be relevant to the specific person):

- they are prohibited from taking business information, when they are no longer associated with the Company
- they agree to comply with the Company's policies, and procedures, including those associated with information security, and protecting business, personal, and sensitive, information.
    - They may be subject to disciplinary action, if non-compliance is identified.

2.10. E-mail

2.10.1. **"E-mail"** is electronic mail, a data message used, or intended to be used, as a mail message between the originator, and addressee, in an electronic communication.

2.10.2. The Company must establish an e-mail privacy statement, approved by management, which statement must be included as part of the e-mail signature of each applicable person.

- Applicable people must ensure that e-mails that they send from the e-mail addresses provided to them by the Company, include the management approved e-mail privacy statement.

2.10.3. Applicable people should only use the Company's e-mail services, including e-mail addresses, and accounts, for business activities.

- However, the Company will allow reasonable personal use of its e-mail, and internet, facilities.
- Management reserves the right to monitor the use, and take disciplinary action, if deemed necessary.

2.10.4. Employees must only use the e-mail address provided to them by the Company, for business related e-mails.

- They must send business related e-mails using the e-mail address provided to them by the Company.

- They must not forward business related e-mails to their private email addresses.

2.10.5. The Company reserves the right to block e-mails sent, or received, from, or to, the Company provided e-mail addresses, which e-mails contain attachments with file extensions that may pose a security threat.

2.10.6. Where applicable people send e-mails that may be deemed to be unsolicited communication, or direct marketing, **EVERY E-MAIL MUST INCLUDE** options to "cancel", "opt-out", or "unsubscribe".

- These e-mails should only be sent to the Company's clients, for financial products, and financial services, offered by the Company.
- These e-mails should not be sent to the Company's clients, who have previously asked to "cancel", "opt-out", or "unsubscribe".
- These e-mails should not be sent to data subjects, who are not the Company's clients, unless they have provided explicit consent to receive this type of communication.
- If E-mail distribution lists/groups are used, to send these e-mails, they must be **UPDATED IMMEDIATELY**, when an instruction to "cancel", "opt-out", or "unsubscribe", is received
- **It is a criminal offence, in terms of the CPA, the ECTA, and the POPIA, to send these e-mails:**
  - **without including options to "cancel", "opt-out", or "unsubscribe"**
  - **to someone who has previously asked to "cancel", "opt-out", or "unsubscribe".**

2.11. Internet and cookie usage

2.11.1. The Company allows reasonable personal use of its internet facilities to employees.

2.11.2. The internet, or internet connections, should not be used to transfer, or download, material that is in violation of laws, including, but not limited to, illegal material, material that violates copyrights, material that contradicts the spirit, and intent, of this Policy.

2.11.3. Applicable people should:

- not provide sensitive information to sources, which are untrusted, via the internet
- not download files from unknown sources, via the internet, because they may compromise information security
- check that secure sites have valid, and unexpired, certificates
- only access the internet via the network connections supplied by the Company.

2.11.4. Employees should access the internet, in accordance with their roles, and responsibilities, including, but not limited to, only:

- downloading files, if authorised to do so
- accessing external systems, if authorised to do so
- using electronic communication technologies to access internal, or external, systems, if authorised to do so

2.11.5. If employees want to publish information on the platforms, websites, or mobile applications, they must obtain prior approval.

2.11.6. The Company reserves the right to restrict access to the platforms, websites, and mobile applications, which may pose a security threat.

2.11.7. The Company's platforms, websites, and mobile applications, may contain links to, and from, the websites of its partners, advertisers, and associates.

- If the visitor follows a link to any of those websites, they must note that those websites have their own privacy policies, and the Company does not accept any responsibility, or liability, for those policies, or how those websites collect, and use, data.

- The visitor should check those policies before they submit any personal information to those websites.

2.11.8. **"Cookie"** is a text file comprising letters, and numbers, that allows the platform, website, or mobile application, owner, to distinguish a visitor's browser/device from another visitor's browsers/device. To learn more about cookies, and how to manage them via a browser/device, the client should visit https://aboutcookies.org/.

2.11.9. The Company, and its third party partners, use cookies on the Company's platforms, websites, and mobile applications, to help manage the sites, and visitor experiences.

- The cookies may be used to collect analytics of non-personal visitor activity outlines, manage personal preferences, provide relevant, or timely, information to the visitor, or offer focused advertisements.
- Cookies, set across the platforms, websites, and mobile applications, by the Company's third party partners, or the Company, may be in the form of session, or persistent, cookies, and may use different technologies, such as JavaScript, or Flash.
- If the visitor wants to 'opt-out' of the cookies, set by platforms, websites, and mobile applications, this can be done on a "cookie-by-cookie" basis, subject to browser settings. The visitor may limit site operation, or functions, if the visitor limits the cookies.

2.12. Network security

2.12.1. The Company must ensure that its networks are adequately controlled, and managed, to protect them from security threats.

2.12.2. The Company must maintain the security of applications, and information systems, which are using its networks, including information in transit.

2.12.3. The Company must identify, and manage, the security features, service levels, and management requirements, of its network services, which details should be included in a network services agreement, regardless of whether these services are provided internally, or externally.

2.13. Physical security

2.13.1. The Company must ensure that work areas at its premises, which contain sensitive information, systems, or services, are appropriately protected by perimeter and/or access control measures.

- Information systems, and the related support equipment, must be secured, and protected for unauthorised access, and other threats.
- Management must approve the access rights to secure work areas at its business premises, which rights should be regularly monitored, reviewed, and updated, as may be necessary.

2.13.2. Electronic files, and data, are backed up daily.

2.13.3. The Company must ensure that the back-up media for the sensitive, and the priority level 1, information systems, are stored securely, offsite.

2.13.4. The Company must, for visitors to its premises, record the date, and time, of the arrival, and departure, of the visitor, together with the minimum personal information of the visitor, so that they can be identified, and contacted, if necessary.

- Preferably, visitors should always be accompanied by an employee, when at the business premises.

2.13.5. Back-up media must be securely transported to the offsite location.

2.13.6. Only authorised management, and IT technicians, are permitted to access back-up media, and restore information systems from back-up media.

2.13.7. The Company must ensure that electrical, and tele-communications, cables that carry data, or support information systems, are protected from interception and/or damage.

2.13.8. The Company must ensure that printed material, containing personal and/or sensitive information is physically destroyed, if not required, or securely stored, if required.

2.13.9. The Company must ensure that personal and/or sensitive information that is locally stored on equipment, is securely overwritten, or deleted, regularly, and before disposal of the equipment.

2.13.10. Management must provide prior written approval for the removal of equipment, software, and business critical information, from its premises.

2.13.11. The Company must ensure that its delivery, and loading, areas at its premises, are isolated from the information processing areas.

2.14. IT compliance, acquisition, development, and installation

2.14.1. The Company must ensure that its information systems, including their design, and operation, and cryptographic controls, comply with the relevant legislative, regulations, generally accepted information security practices, international best practice, contractual (including licence agreements), and business, requirements.

- Management must ensure that the information systems are regularly assessed, and monitored, to determine the level of compliance.
    - Remedial action must be taken, within specified timeframes, to rectify non-compliance.

2.14.2. The Company must ensure that its information system audit/monitoring tools are appropriately protected.

2.14.3. The Company must ensure that the business requirements for potential new information systems include the appropriate information security controls, in terms of this Policy, and related policies.

2.14.4. The Company must ensure that appropriate governance, and validation, controls, are implemented, to verify the accuracy, applicability, and validity, of data that is input into, stored within, and output from, information systems.

2.14.5. The Company must ensure that the IT technicians have documented procedures in place, to control, and monitor, the correct installation of approved software on devices.

2.14.6. When the Company changes its operating systems, or other information systems, it must ensure that priority level 1 information systems are reviewed, and tested, to ensure that there is no adverse impact on business operations, or information security.

- Documented change control procedures must be in place.

2.14.7. When information systems are tested, the applicable people must ensure that the test information is carefully selected, used, and controlled, to ensure the protection of personal information.

2.14.8. The Company must ensure that the source code of information systems is restricted to authorised people only.

2.14.9. When software is developed by third parties, the Company must ensure that the appropriate confidentiality, and service level, agreements, are established.

- The development must be supervised, documented, and monitored, by designated employees of the Company.

2.15. Business operations

2.15.1. The Company must apply appropriate procedures, to assess the fitness, and propriety, of potential, and existing, employees, applicable to the roles, and responsibilities, of the specific person.

2.15.2. The Company must ensure that business processes, and procedures, including the processes, and procedures, for using information systems, are documented, and are updated whenever required.

2.15.3. Management must ensure appropriate segregation of roles, and responsibilities, to reduce the risk of loss of, damage to, or unauthorised destruction of, business, personal, and sensitive, information, and unlawful access to, or processing of, business, personal, and sensitive, information.

2.15.4. The Company must ensure that information security risks are continuously assessed, and that business, and information security, controls, processes, procedures, and policies, are updated whenever required.

2.15.5. The Company must ensure that its employees are always appropriately trained, and supervised, about the applicable legislation, regulations, controls, processes, procedures, and policies, including those related to information security, and protecting business, personal, and sensitive, information.

2.16. Electronic signatures and transactions

2.16.1. The Company must ensure that the information involved in electronic transactions, passing over public networks, is appropriately protected from fraudulent activity, contractual dispute, unauthorised disclosure, modification, or deletion.

2.16.2. The Company must ensure that information involved in online transactions are appropriately protected from incomplete transmission, mis-routing, unauthorised message alteration, disclosure, duplication, replay, or deletion.

2.16.3. The Company must ensure that the integrity of information available on publicly available systems, is appropriately protected, to prevent unauthorised access, disclosure, modification, or deletion.

2.16.4. The Company permits documents, and agreements, to be signed by hand (in ink), digitally, through marking a check/tick box, or digitally, through an electronic signature, unless prohibited, or restricted, by legislation.

- **“electronic signature”** is data attached to, incorporated in, or logically associated with, other data, and which is intended by the user, to serve as a signature.

2.16.5. The Company permits agreement to be executed in counterparts, each of which will be an original, and which together constitute the same agreement.

- Signature of the agreement, by the parties, sent electronically, by fax, email, or by electronically accepting the terms and conditions on our platforms, websites, or mobile applications, will be treated as the party`s original signatures, for all purposes under this agreement.
- Sending copies of the agreement, and the pages requiring signatures, by fax, email, in “portable document format” (“.pdf”) form, or by any other electronic means, intended to preserve the original appearance of the agreement, or by a combination of these methods, will be effective execution, and delivery, of the agreement, to the parties, and may be used as an original agreement, for all purposes.
- The parties record that it is not required for the agreement to be valid, and enforceable, that a party shall initial the pages of the agreement and/or have its signature of the agreement verified by a witness.

2.16.6. **Where legislation provides for agreements to be signed electronically, but does not specify the type of signature, the requirement in relation to a data message is ONLY MET IF an advanced electronic signature is used.**

- **"advanced electronic signature" (AEA)** is an electronic signature, which results from a process that has been accredited by the Authority (.za Domain Name Authority).
- This AEA requirement is causing the electronically signed agreements of financial institutions to be non-compliant with the ECTA, where financial institutions are not requiring the electronic signatures of clients to be AEAs.
- Examples of affected legislation are the Collective Investment Schemes Control Act 45 of 2002, and the Financial Advisory and Intermediary Services Act 37 of 2002.
- The Financial Sector Conduct Authority has been made aware of this non-compliance, and since electronic transacting supports easier access for clients, and is supportive of financial inclusion, it **MAY EXEMPT** certain financial institutions from the AEA requirements, **IF** the electronic signature, and the obtaining of the electronic signature, meets certain criteria.

2.16.7. The Company must ensure that the permitted electronic signature complies with:

- The client must sign the electronic agreement, by way of an electronic signature.
- The Company must verify the identity of the client, and implement processes to authenticate each transaction of the client.
- The agreement must provide for:
  - conditions of submitting the electronic agreement
  - procedure for submitting the electronic agreement
  - terms and conditions applicable to submitting the electronic agreement, and the legal implications thereof
  - disclaimers of liability on the part of the Company
  - limitations of liability applicable to the Company
  - security risks, and risk of interception, inherent to electronic transacting
  - related precautionary, or security, measures
  - confirmation by the Company that its website complies with relevant legislative requirements applicable within South Africa.
- The Company must ensure that the terms and conditions under which an electronic agreement may be submitted, **MUST BE DISPLAYED on the screen of the digital platform being used to submit the agreement**.

2.16.8. **Refer to the terms and conditions for details about transactions.**

3. Commencement, and termination

3.1. Notwithstanding the last date of signature of the agreement, the agreement commences on the date that the Company has completed the initial customer due diligence procedure, accepted the business relationship, signed the agreement, notified the client that it has accepted the business relationship, provided the client with the relevant bank account details, into which they must deposit funds, they have deposited funds into the relevant bank account, they have notified the Company that the funds have been deposited into the relevant bank account, and the funds are reflected in the relevant bank account.

3.2. The agreement will, subject to the provisions specified therein, commence on the commencement date, and will continue indefinitely, until terminated by not less than thirty (30), and not more than sixty (60), calendar days' written notice, by either party, to the other.

3.3. On termination of an agreement, the Company will complete any transactions that it started, on the client's behalf, before receipt of the notice of termination.

3.4. The Company will not start any transactions, on the client's behalf, after it has received, or given, notice of termination, unless the client instructs it to do so.

3.5. Upon termination of the agreement, the Company will return all monies, financial products, and documents of title, to the client, and will provide the client with a detailed final statement of account.

3.5.1. If the financial products, and documents of title, are in possession of an approved nominee, the relevant administrative financial services provider (administrative FSP), or its independent nominee,

the Company will issue an instruction to the relevant nominee, or administrative FSP, to arrange that the financial products, or documents of title, be returned to the client.

3.6. Refer to the agreements, and terms and conditions, for details about the commencement, changes to, and termination of, agreements.

4. Payments and refunds

4.1. Payments are not made online, through the Company's platforms, websites, or mobile applications.

4.2. The Company makes the following payment methods available to clients:

4.2.1. Electronic fund transfers, or secure internet deposits

4.2.2. Debit orders

4.3. Clients are only provided with the relevant bank account details once the Company has accepted the business relationship, or single transaction.

4.4. Generally, the Company only accepts payments directly from the client (i.e. not from third parties). However, may be assessed by management, depending on the circumstances of the case.

4.5. The Company does not accept cash payments, and does not make cash payments.

4.6. Cooling off periods are only applicable to certain financial products.

4.7. Generally, refunds are not permitted. However, may be assessed by management, depending on the circumstances of the case.

4.8. Refer to the terms and conditions for details about the payment methods, and refunds.

5. Consequences of non-compliance with the policy

5.1. All employees are obliged to comply with the Policy, and it is a condition of employment. Non-compliance is a breach of their employment contract, and is an action of misconduct, so employees may be subject to disciplinary action, which may lead to dismissal. Non-compliance by an employee will be dealt with according to the Company's disciplinary policy. For assessing, and addressing, the non-compliance, reports made by the compliance officers, internal audit, external audit, and the Authorities, will be considered, for appropriate action to be taken.

6. Policy review

6.1. The policy will be reviewed at least annually, updated, if necessary, and the latest version will be adopted, and approved, by the board.