INFORMATION, COMMUNICATION & TECHNOLOGY GOVERNANCE & USAGE POLICY

OBJECTIVES WITH THE ICT POLICY

Protecting our intellectual property and financial data
Meeting our regulatory and legislative obligations
Demonstrating to our suppliers and clients that we are serious regarding security

GUIDING PRINCIPLE

The responsibility of governance rests in the Board of the business. The Board mandated the senior management of the business to implement the requisite policies and procedures to ensure technology and information security governance. It is the responsibility of every company employee to adhere to the provisions of this, and other, information and technology governance policies and procedures.

The technology facilities and information resources are the property of the business and not that of any individual. These facilities must therefore, except where rules are specifically relaxed or limited, be used for company business and to advance the interests of the company. This policy is applicable to employees and users (where a user is a person that accesses the company electronic installation as a consultant, contractor, etc.).

1. USER ACCESS & PASSWORDS

Passwords are one of the most important aspects of computer security. Poorly chosen passwords or failure to manage passwords may result in unauthorised access and could lead to the theft of information or other forms of fraudulent activity. This could severely damage the company financially or tarnish its reputation. All users, including contractors and vendors with access to the company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure passwords to safeguard the integrity of the company's electronic installation.

The following general protocols apply to passwords:

- All passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- No person may duplicate personal use passwords for any business account or access.
- All passwords must conform to the guidelines described below.

Employees must choose strong passwords. Passwords therefore should have the following characteristics:

- May not be guessable (password, password2020, gustav20, etc.)
- May not be linked to personal information (birth dates, spouse's name, child's name, etc.)
- Should be a mix of characters (contain special characters, uppercase, numbers, etc.)

Password Protection

- All passwords are to be treated as sensitive and confidential company information.
- Users may under no circumstances share passwords with any person.
- Passwords may never be written down or stored on-line without encryption.
- Passwords may not be revealed in any email, chat, or other electronic communication.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Always decline the use of the "Remember Password" feature of applications (e.g., Outlook).
- If an account or password compromise is suspected, report the incident to the KI.

2. ELECTRONIC MAIL

As the recipient of any mail may view any email message as an official policy statement from the company, mails may not compromise the company in any manner. All emails sent or forwarded by a user must therefore be appropriate and not bring the name or image of the company into disrepute.

2.1. All use of email must be consistent with the company principles of ethical conduct and must comply with applicable laws and proper business practices.
2.2. Any company email account should be used primarily for business-related purposes; personal communication is permitted on a limited basis but mails for personal commercial gain are prohibited. Any user may use a reasonable amount of company resources for personal emails and personal business, but emails not related to the business of the company must be saved in a separate folder from work-related email.
2.3. It is prohibited to send chain letters or joke emails from a business email account.
2.4. Emails may not be deleted, changed, destroyed or removed from the company server if such mail in any way relate to the business of the company (subject to the provisions of the Data Retention Schedule).
2.5. The company email system may not to be used for the creation or distribution of any offensive messages, including comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Users who receive any emails with this content from any other user must immediately report the matter to senior management. A user may also not forward or distribute such offensive messages.
2.6. Employees may not use any personal drive for sharing or storing company information. This includes sending or receiving company-related information via G-mail or a similar personal address.
2.7. Employees are required to double check the names of recipients of mails and ensure they do not send ANY mail to a person not intended as the recipient.
2.8. Individual messages which are forwarded by any employee may not contain company confidential information, except where the employee is specifically authorised to share such information (for example financial information with the company accountants).
2.9. Employees must always ensure they send, where prescribed, client information, policy details, or other personal information using passwords or encryption. Where any message is password-protected, the password may not be sent to the receiving party by mail but must be sent by text message.
2.10. Company employees and users shall have no expectation of privacy in anything they store, send or receive on the company's email system.
2.11. The company may monitor messages without prior notice and may access the computer of any user to conduct such monitoring.
2.12. The company may access the company assets allocated to any employee for investigation purposes and an employee may not refuse access to such asset (for purposes of the Policy a Company Asset includes any company issued phone, notebook computer, personal computer, storage device, etc.).

3. USE OF TELEPHONES AND DATA

3.1. The provisions of Section 2 shall apply to the use of mobile phones and mobile phone applications as it relates to misuse of technology when wasting time during company hours, sending and receiving prohibited material, sending or receiving confidential material, advancing own interests, etc. This prohibition is not restricted to company-owned devices but includes own devices, used on company time or on company premises.
3.2. The company may at any time access the company phone of any employee or user to determine whether the device or any application loaded thereon was misused or used for any of the prohibited practices.
3.3. No pictures may be taken of any company document and no pictures of company documents or information may be sent to third parties.
3.4. An employee may not use any cellular phone to conduct company business, except where the employee was specifically authorised to conduct such business. This includes sending or receiving business-related mails on own phones or company phones.
3.5. Where an employee receives information of a client (such as pictures of identity documents) by what's app or any other similar application, the employee must immediately ensure such information is saved to the company technology infrastructure and deleted from the device and account it was originally sent to.
3.6. The company will take disciplinary action in the event an employee or user sends prohibited materials from any device and irrespective of whether it is to a co-worker, contractor, vendor or any other external party.

4. INTERNET USE

The brokerage is a responsible employer and trusts its employees and contractors to use the internet and facilities in a sensible way and not waste time and resources. The company will therefore allow reasonable access to the internet other than for company use. If this privilege is abused restrictions may be imposed on specific users and, in the case of gross mismanagement of time and resources, disciplinary steps will be instituted.

The principles under Section 2 also apply to using the internet. In addition, the following is specifically prohibited:

4.1. It is prohibited to visit sites that contain obscene, hateful or other objectionable material. Users may not make or post indecent remarks, proposals, or materials on the internet.
4.2. Users may not subscribe to anything on the internet that does not support the work being performed for the company.
4.3. Users may not visit chat rooms that are non-work related.
4.4. Playing online games is strictly prohibited.
4.5. The upload, download, or otherwise transmission of commercial software, programs or any copyrighted materials belonging to parties outside of the company, or the company itself, is also forbidden.
4.6. No free software or programs may be downloaded onto a company device.
4.7. No software or programs installed on a device may be altered or modified in any manner.

5. CLEAN DESK, CLEAN SCREEN AND OTHER SECURITY PROVISIONS

This section of the policy is necessary to reduce the risks of unauthorised access to, or loss of, or damage to, company information. All users are required to observe the protocols contained in this section to minimise unauthorised access to or loss of information.

5.1 Employees are required to ensure that all sensitive/confidential information in hard copy or electronic form is secure in their work area at the end of each workday or before they go on leave or travel on behalf of the company.
5.2 Computer screens must be locked when the person is not at his/her desk.
5.3 Computers must be shut down completely at the end of each workday.
5.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied. The same protocol applies at the end of each workday.
5.5 Filing cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
5.6 Keys used for access to Restricted or Sensitive information may not be left at an unattended desk.
5.7 Laptops and other portable equipment must be locked away in a drawer or cabinet when not in use.
5.8 Company equipment (such as phones or laptops) taken offsite for any purpose must always be kept secure and may not be left on a seat or in plain sight in the vehicle when driving or when the vehicle is parked. Vehicles containing company equipment may not be parked in dark or unsafe areas.
5.9 Laptops taken home must always be kept secure when at the employee or user's home.
5.10 Printouts containing Restricted or Sensitive information must immediately be removed from the printer.
5.11 Upon disposal all documents must be shredded in the official shredder bins or placed in the confidential disposal bins.
5.12 Whiteboards containing Restricted and/or Sensitive information must be erased.
5.13 Mass storage devices such as CDROM, DVD or USB drives must be treated as sensitive and must be secure by storing in a locked drawer or similar safe place (such as on the body of the person). Such devices may not be left at printing facilities, internet café's, restaurants, clients, etc.
5.14 Where a company device or personal device, containing company information is lost, the loss must within 24 hours be reported to management.

6. INFORMATION SENSITIVITY AND CLASSIFICATION

Any information about persons or other businesses that are collated must be stored in a secure manner and may not be disseminated in any way that would contravene the Protection of Personal Information Act or the FAIS General Code.

Employees must familiarise themselves with the information classification of the company. The company has three types of information: public, company confidential and client confidential. Sensitivity levels are guidelines created to protect company and client confidential information. It is not designed to impair daily activities but to assist users in deciding what information must be protected.

Public information is information that has been declared public knowledge by someone with the authority to do so and can freely be given to anyone without any possible damage to the company. This generally consist of general corporate

documentation, brochures, documents available from public records, news items, advertisements, etc. This type of information is generally accessible through application in terms of the Promotion of Access to Information Act Manual.

Client confidential information is particularly confidential and may not be disseminated in any manner that contravenes the POPI Act or any agreement or undertaking given to that client (corporate or individual client).

Company confidential information is sensitive (secret) and must be protected. Included is information that must be protected very closely, such as trade secrets, development programs, potential acquisition targets, financial information and other information integral to the success of our company.

All confidential information must be secured and may not be disseminated except where disclosure is required by law (e.g. returns or statistics), disclosure through agreement with a third party (e.g. financial information required for a merger) or in terms of a court order (e.g. litigation with a supplier). In general terms confidential information may not be disseminated upon request except where senior management authorises disclosure.

Information security is further dealt with in the following policies:

- Protection of Personal Information Policy;
- Employment contract & undertakings; and
- The FAIS Compliance Policy.

7. EXTERNAL STORAGE & REMOVABLE DEVICES

Employees and users are not allowed to make backups of information or copies of any document (including reports, client lists, contact details, address lists, photographs, graphs, etc.) onto a device that is not authorised by management. No such copies may be made without express prior consent of management.

To ensure the integrity of the company information and communication infrastructure, it is prohibited for any employee or other user to perform any form of storage outside of the company's domain, such as on Dropbox, Google Drive, etc. The company will not authorise an employee to make use of such a storage drive. The company will not authorise any employee to use personal mail addresses for sending and receiving business-related mails.

No removable drive (CD ROM, thumb drive, memory card, etc.) may be introduced into the network or any device that forma part of the company's electronic installation without management's prior consent. Any such device containing company information must always be kept secure (refer Section 5 for details). The company closed all computer ports for removable drives.

8. BACKUP POLICY

It is required of all businesses to retain data in a secure manner. Companies must be able to recall information stored and recover from a disaster on an individual (loss of a computer) or enterprise wide (loss of data through a virus) basis. Employees and users (if required to comply with this prescript) must therefore adhere to the company backup prescripts as to timing and extent of backups.

The details of the backup policy and plan is as follows:

FREQUENCY	WEEKLY/MONTHLY
METHODOLOGY	BACKUP BY CEO TO LAPTOP AND EXTARNAL HARDDRIVE
BACKUP PROGRAM	-
BACKUP PROVIDER	-
STORAGE OF BACKUPS	CEO LAPTOP AND EXTERNAL HARDDRIVE
ALTERNATIVE STORAGE	EXTERNAL HARDDRIVE
RECOVERY METHODS	ATS
CONTRACTS IN PLACE	-
FREQUENCY OF TESTING	

9. INFORMATION SYTEMS & SECURITY

The following describes the systems and programs employed by the company:

NUMBER OF COMPUTERS	5
NUMBER OF PRINTERS	6
SERVER IN USE	1
PROGRAMS INSTALLED	
FIREWALL INSTALLED	KASPERSKY
ANTI-VIRUS PROGRAM	KASPERSKY
IT SERVICE PROVIDER	ATS
MAINTENANCE CONTRACT	-
HARD COPY STORAGE	2

10. DATA RETENTION & DESTRUCTION PRESCRIPTS

All records must be stored for the periods prescribed in law. For a breakdown of these minimum retention periods, refer to the legal compliance matrix as set out in Annexure A. Records may not be destroyed before the prescribed dates.

The company must have good reason to store any record beyond the prescribed retention dates, especially where it relates to personal information of clients, employees, etc. and the data can no longer be retained as it would be outside scope of the collected purpose specification. Such data must be de-identified as prescribed in the POPI Act. Senior management must sign off the retention of information after the prescribed retention date expired.

Destruction of hard copy information can only take place once it has been safely taken up in the company information system in a digital format (such as a digital copy, photograph, minutes of meeting, etc.). Such information must always be safeguarded to ensure that it cannot be accessed by persons not authorised to receive it, access it or copy it. Where indicated files may be encrypted for certain persons gaining access to it using a password or other form of identification.

Some secret and confidential information may have to be expunged from digital sources which includes destruction of discs, formatting of hard drives before selling or writing off equipment, etc.

11. ENFORCEMENT AND DICIPLINE

11.1 Any employee or other user who fails to adhere to any duty conferred by this policy or that transgresses the policy in any manner will be subject to disciplinary measures that may lead to his/her dismissal or termination of his/her contract.

11.2 Certain transgressions as contained in this policy constitute criminal behavior and the brokerage may be required by law to report such transgressions for criminal investigation and prosecution.

11.3 The theft, misuse, proliferation, etc. of client information exposes the company to risk of regulatory action. Any person who is guilty of any activity relating to client information in contravention of the Protection of Personal Information Act, FAIS Code or the Policyholder Protection Rules (issued in terms of the Long- or Short-term Insurance Act) will be subjected to reporting to the relevant authorities and may face dismissal, debarment and/or prosecution.

11.4 Transgressions as contained in this policy may cause an offender to be liable in terms of civil law and exposes such person to civil actions for damages that may be instituted by the company or a third party.

ANNEXURE A: RECORDS RETENTION SCHEDULE

Personal information as provided for in POPI	
Personal information of consumers, business partners, etc. may be collated and retained with the consent of the person or may be prescribed by law. Records must be safeguarded and may not be disclosed or disseminated or used without consent of the person. It may not be retained indefinitely and must be returned, deleted or destroyed if no longer required or necessary.	Subject to requirements in other applicable legislation records may not be retained longer than necessary to achieve the purpose of collection.
Auditor engagements	
Engagement documents and working papers	5 years from issuing the audit report
Close corporations	
All accounting records	15 years
Founding statements and amendments (CK 1 & 2)	Indefinite
Annual financial statements	15 years
Minute books and records of resolutions	Indefinite
Companies	
All documents and accounts	At least 7 years
Notice of Incorporation, MOI, Rules, Registers, etc and all changes thereto	indefinite
Records of shareholder meetings including notices, minutes and resolutions passed	At least 7 years
Annual general meeting: all reports considered & all other records	7 years
All accounting records and annual financial statements	7 years
Records of directors and former directors (to retain after retiring/resigning)	7 years
Minutes and other records relating to meetings of directors or any committee formed by the board	7 years
Register of securities and all records relating to changes in shareholding	Indefinite
Consumer Protection (if CPA applies to business)	
All information provided or disclosed to the consumer	3 years
Credit records (if NCA applies to the business)	
All records relating to applications for credit including declined applications and reasons for declining, payment records, steps taken to recover debt, etc.	3 years from date record was created or delivered to the consumer
All financial, operational and other business records of the credit provider including application to register	3 years from date the record was created
Any dispute lodged by a consumer and records of how disputes were dealt with	6 months from date of finalisation
Electronic communications and transactions (ECT Act)	
Personal information collated, processed and stored by any person o behalf of another person	At least 1 year after purpose of collation falls away
Obsolete information	Destroy when it becomes obsolete
Financial services records (FAIS Act)	
All transactions records with a client, including advice records, cancellations, non-compliance records, complaints, compliance by representatives, etc.	5 years from termination of client relationship
Transaction records where the client enters into a single transaction with the business	5 years from date of conclusion of transaction
Records of representatives and key individuals	If resigned for as long as employee records must be retained
Financial Intelligence Centre compliance	
Records relating to risk rating of a client, client take-on records, transaction records, etc.	For period the person remains a client and then for a further 5 years
Transaction records where the client enters into a single transaction with the business	5 years from date of conclusion of transaction

Transaction records relating to the reporting of suspicious and unusual transactions	5 years from the date on which the report was submitted to FIC
Health & Safety records	
Records of earnings of employees and records that must be retained for all employees (refer BCEA prescripts)	4 years after an entry made in a record or employee resigned
Records of treatments of an employee (more than basic first aid) injured in any work-related incident	3 years from date of incident or 3 years from date of last treatment
Records of Health & Safety Committee meetings, including reports and recommendations delivered to the employer	3 years from date of meeting or of delivery of report
Employment records	
The Basic Conditions of Employment Act prescribes certain particulars of all employees to be recorded and retained. This includes: - Personal information - Job title or occupations - Time-keeping records - Remuneration	For period of employment until 3 years after termination
All information relating to the employer's workforce and steps taken to comply with the Employment Equity Act	5 years
The Employment Equity Plan of the business as well as all amendments thereto	5 years after any plan comes to an end
Annual Employment Equity Reports submitted to the Director-General	5 years after submission of a report
Disciplinary records, including charge sheets, records of outcomes and dismissals	Indefinite
All UIF returns as well as statutory records returns are compiled from (payroll information that includes personal details of employees and remuneration details)	5 years from date of any return or compilation of record (recommend 7 years)
Tax compliance & tax records	
Any tax return and all information a return is compiled from (companies tax, provisional tax, employees' tax, etc.)	5 years from date of submission
In the event of duty to submit a return but the business failed to submit the return before the date it was due	Retain until submission and for 5 years thereafter
If any exemption to pay tax is applied for but generally a tax return or payment would have been due	5 years after the end of the tax period the monies were earned
Employee tax records including remuneration records, taxes withheld or paid over and income tax numbers of each employee	5 years from date of submitting a return (such as an EMP201)
Registered micro businesses (turnover consistently under R1 000 000) must retain records of income received, dividends declared, assets worth more than R10 000 at purchase and each liability in excess of R10 000.	5 years after date return is due after end of a particular tax year
VAT returns and all source documents (evidence) the return was compiled from	5 years from submission of the VAT return
Evidence (including payment records, method of valuation, number of shares, etc.) of transfer of an unlisted security by a company or transfer of interest by a member of a close corporation	5 years from date of transfer of the security or interest