COMMUNICATION AND CONFIDENTIALITY POLICY

*A data protection impact assessment must be conducted where any change to the policy will include risk to personal information e.g new systems, transfer of information, new providers

This policy is intended to guide staff to meet the organisation's communication and confidentiality measures and obligations.

APPLICATION

This policy applies to all Staff

INTRODUCTION

Our organisation is very careful to ensure that we have proper communication channels, and encourage openness and honesty, whilst still respecting the confidentiality of the organisation's as well as all our customer and suppliers' personal or confidential information. All persons need to be aware that there is national legislation that covers this area.

To ensure that the organisation complies with the applicable legislation and maintains customer confidentiality, there will be nominated liaisons between external parties and the firm.

This document provides guidance on what to do when receiving requests for information from regulators, law enforcement bodies and third parties. It aims at ensuring that customer confidentiality is maintained whilst still complying with all applicable legislation and protecting our business reputation.

APPLICABLE REGULATION

- POPI
- Consumer Protection Act
- National Credit Act
- Contractual obligations

RISK

This policy addresses the risk of information which is confidential being disclosed to unauthorized persons.

Risk Tolerance: Low.
The organization is not prepared to accept any risk and effective mitigation must be in place.

POLICY

Personal information and confidential information must be kept secure, disseminated on an approved basis only, and confidentiality maintained at all times.

Information may only be shared with approved persons and accessed by authorized individuals.

Personal information

- Privacy of the individual's details must be maintained at all times.
- Personal information that needs to remain confidential includes the age, gender, address, ID, date of birth, financial information, or any other information of a personal nature of the individual.
- Other topics that also need to remain private are details of health issues, family information. Any other information of a personal or sensitive nature should be discussed only with the appropriate people when and where others will not overhear the conversation.
- Persons sometimes will discuss details of a person in the lift, in the corridor or in the tearoom; this is a policy breach.

Communication with regulators, other third parties and the media

Requests from regulators or law enforcement bodies

Regulators must be dealt with professionally, promptly and in a centrally coordinated manner. This includes requests from:

- Financial Regulator
- Credit Regulator
- South African Reserve Bank
- South African Police
- South African Revenue Services
- Hawks, other external parties e.g., attorneys, subpoenas, requests in terms of any law such as Promotion of Access to Information Act etc.

The following procedure must be followed when requests for information from any of the above parties are received:

1. Immediately direct the request to the nominated representative, within 24 hours of the request being received;
2. S/He will assess the request and ensure that all details are applicable with the nominated legislation;
3. S/He will confirm and verify details and authority of the requester;

4. S/He will consult with the required business units within the firm;
5. S/He will compile the required information;
6. S/He will submit the information to the requester;
7. The Information dealing with the request will be captured on the firm's database.

External (media) communications policy

Communication with the press must be handled in a professional and coordinated manner and ensure that the firm's position is fully explained and as accurately reported as possible.

No employees are allowed to talk to the press about matters relating to the firm, or respond to enquiries from journalists, without the prior approval of the firm's CEO unless they are on the approved list of spokespeople.

Never give information to the press or media. There is always a spokesperson for the organization that will be designated as the person to speak with them.
Politely decline any requests and refer the person to a supervisor.

Appointed spokespeople must only discuss subjects within their own expertise. Management must confirm the approved spokespeople.

Under no circumstances should employees discuss with the media any of the following matters:

1. The affairs of any customer
2. Whether or not a particular customer has engaged the firm, unless this engagement has already been publicly announced or customer consent has been obtained
3. The affairs or practices of the firm
4. Pending or possible litigation involving the firm
5. Current or former employees

Release of information

Normal requests in the course of business (For example: requests for customer or policy information)

Before releasing any information to auditors, accountants or any other third party, whether verbally or in writing, you must ensure that you are entitled to release such information and obtain the client's or client's authorized signatory's approval.
The onus of ensuring that you know your client/ talking to your customer or/and obtaining written authorization rests with the organization. Unless you identify beyond doubt the person's voice, you may not release any customer or policy information telephonically.

Any request other than made in the normal course of business must be referred to Compliance or the appointed person nominated in the Register of Roles. The same applies if you are in doubt as to the nature of the request or as to the person requesting the information.

Telephone

- The only time transfer of information is appropriate over the telephone is between authorized persons. Authorized persons will give their details to verify their identity and obtain verification of the person to whom they are speaking.
- When answering the phone, don't ever give out any information unless you are authorized to do so, and only after you are sure of the person's identity and authorization to receive this information. If this is not forthcoming, refer the enquiry immediately to a supervisor, manager or authorized person.
- If you are ever in any doubt as to the caller's identity, or suspect that something is not right, inform a supervisor immediately and do not comply with any requests from the caller.
- Ensure full notes/ records are kept of all calls

Personal responsibility and communication guidelines

Individuals are personally responsible for the safe-keeping and appropriate restriction of information which flows to them during the course of their employment. Managers in particular must act with due diligence when disseminating reports and other information on a "need to know" basis and must undertake the periodic destruction of obsolete or outdated records.

Managers are responsible for ensuring that a properly designated and maintained system of records is implemented and must regularly review the system's integrity and confidentiality in order to maintain the standards required by this confidentiality policy.

The business' working relationships with many outside consultants, suppliers, vendors and other stakeholders demand a large measure of disclosure of information. Discretion must be exercised in terms of the type and frequency of the information that is being shared. Consultants, in particular, are appropriately treated as business "partners" in this regard and it is incumbent on the hiring manager to ensure that all such consultants sign a confidentiality agreement prior to embarking on the project for which they are hired.

All persons, contractors and other personnel employed by/ mandated by the business are required to treat all customer and business information with the utmost confidentiality. Persons with access to confidential, private or sensitive information are not allowed to divulge this information with any other persons unless authorized to do so.

If you are ever asked to divulge confidential information about a customer by a person who has no authority to request this, please report the matter to your supervisor immediately.

If you ever hear an employee/contractor etc. discussing information of a confidential and/or private nature in an inappropriate way (eg, chatting to a colleague in the office or lunchroom, telling friends in a social setting), you must report the matter to your supervisor/KI immediately.

The easiest way to follow this policy is to remember one simple rule: NEVER give out confidential and/or private information about a customer unless it's to an authorized person. This means not even to family members - we have no way of knowing a person's family situation, and that person has the right to withhold private information from his/her family members.

The business takes the confidentiality and privacy of our customers very seriously and will not hesitate to take disciplinary action against any persons that are in breach of this policy.

CONFIDENTIALITY RULES

All employees/ contractors/ mandatories must have a confidentiality clause inserted into their contracts of appointment. Irrespective of whether such a clause is included in any contract, the provisions of this policy apply mutatis mutandis and form part of the terms and conditions of appointment.

The appointed person acknowledges that in the course of rendering services in terms of this Agreement he will acquire or receive information of a confidential nature, including, but not limited to information relating to the business of the Employer/Mandator, Product suppliers, or customers.

PROHIBITED

The following is not permitted (during the course of appointment, or at any time afterwards). No person may:

- use or disclose or allow third parties to use or disclose any confidential information
- be entitled to information regarding a customer's portfolio without the customer's written consent
- if requested, the appointee must provide the organization with written proof of the customer's consent immediately when requested to do so
- the provisions of this section survive the termination of the appointment

Any unauthorized disclosure of any information concerning:

The organization's results, methods, procedures, names and structural arrangement with suppliers or customers, ideas, research, software and hardware in use in computer operations and applications, any relevant data which is either being used or will be used by the firm, as well as any other matter or information which is not readily available in the ordinary course of business to a competitor or potential competitor of the firm, will constitute a breach of contract, unless you are required by law to disclose such knowledge.

No person may at any time either during or after this appointment, divulge or disclose any matters connected with this appointment (except those matters which are, or by their nature shall be, matters in the public domain) to any persons or entity without the consent in writing of the firm

Any breach of the above is a compromise of the honesty and integrity of the person in question and appropriate action will be taken by the organization in any such instance

RAMIFICATIONS OF BREACHES OF THE CONFIDENTIALITY OF RECORDS

In a situation of this policy being breached, a customer can take legal action against the person as well as the entity responsible. Our business owes a duty of care to the customer to prevent any "damage" to the client.

To avoid a successful claim by the client, we must be able to prove that we have steps in place to prevent such a breach taking place. These steps are:

- Recruitment and selection of persons/mandatories or contractors, incorporating background checks
- Induction training of new persons on confidentiality and privacy and record keeping policy and procedures.
- Annual training, reinforcing our policies and informing people of any changes to policies.
- Correct audited procedures for record keeping.
- Security systems in place to monitor and record computer access to information.
- Security systems in place to regulate the level of access to information for different persons.
- Security systems in place to prevent data breach
- The police are called in if there appears to be any breach.

If our policy and procedure regarding confidentiality of customer information is not followed, the individual person will be liable to disciplinary action, which may lead to dismissal, debarment or lawsuits.

ALL persons, mandatories and contractors are required to sign a confidentiality agreement when they commence employment or mandate. This is a legally binding document that clearly states your obligation to treat all customer information in a confidential manner.

ACCESS TO RECORDS

Records may be paper, or computer based, stored on discs or CDs or on smart devices. Records have legal, administrative and cultural constraints on their storage and disposal.

- Persons do not all require the same level of access to information. The level of access required is determined by the person's role.
- Security access may be issued whilst the person is working on a particular job, and then withdrawn if the level of access required changes.
- Persons require ID access or an electronic door pass to access data.
- Computer access and content is monitored and restricted to ensure that customer confidentiality is maintained
- No unauthorized copies of any information may be held or made, and no unauthorized information may be transferred onto a personal device (cellphone, iPad, laptop)
- Any personal information or confidential information which is legitimately held on e.g. A memory stick, must be password protected and encrypted
- Documents need to remain private and confidential and must at all times be stored in a securely locked cabinet for access by authorized personnel only.
- Documents are not to be left where members of the general public, or any other unauthorized person may access them as the information within them could be taken out of context or made public.
- Check with and obtain the written consent from a person prior to allowing family members to access documents. There may be information that the customer does not wish their family, friends or others to know.
- Customers are able to access their own information once their identity has been verified.

INTER-ORGANISATIONAL ACCESS

Records may not be transferred from one organization to another without written management approval. Not all organizations have reciprocal privacy agreements, so care needs to be taken and the correct channels followed to ensure that any sensitive or confidential information is not passed over to someone that may not treat the information in the same confidential manner as your organization.

COMPUTER AND INTERNET CONFIDENTIALITY

- Within an organization there will be information that is sensitive and confidential in nature stored on the computer network.
- All computer equipment must be password protected, and no passwords may be shared or disclosed with any other persons
- At no time are persons to allow access for visitors to view computer-based information. Information that is printed out must be filed in the appropriate place according to the firm's protocols.
- Any information that is to be discarded must be thrown into the locked bins for shredding prior to being discarded.
- All information stored electronically must be permanently destroyed, with no possibility of data recovery, when destroyed
- All information stored electronically which is no longer required for its purpose must be removed and either archived or destroyed according to the recordkeeping policy.

CHANGE

This policy may be changed after assessing the impact and ensuring that change is in the interest of the Company and does not present any unacceptable risk. All changes must be approved prior to implementation.

NON-COMPLIANCE

Non-compliance with this procedure may lead to disciplinary action e.g. [up to and including dismissal]