Access Bank South Africa

Protection of Personal Information Act

Level 3

2021/05/25

Document control		
Version:	e.g. V2-2020	
Category /level	Category 0 / Level 3	
Date of the last review:	February 2019	
Author:	Adopted from Edward Nathan Sonnenberg Attorneys	
Owner:	Information Officer	
Reviewed by:	Reviewer Name or Committee	Reviewer or Chairperson of Committee signature: _____ Date: _____
Approved by:	EXCO	EXCO Chairperson signature: _____ Date: _____
Noted by:	BOARD (Category 1 Only)	BOARD chairperson signature: _____ Date: _____

Category 0 Policies based on South African legislation, for notice to Access Bank PLC.
Category 1 Policies require Access Bank PLC approval and Access Bank (SA) Board approval
Category 2 Policies requires Access Bank (SA) Exco and Access Bank PLC approval

Level 2 Policies belong to Access Bank Plc
Level 3 Policies belong to Access Bank SA

TABLE OF CONTENTS

A. Purpose

The purpose of the policy is to establish management direction and high-level objectives for regulating the manner in which personal information is processed and to provide for remedies in cases where personal information is not handled accordingly. Further purposes of the policy include:

1. the supplementation of Access Bank South Africa and to align it with South African laws;
2. compliance with the requirements of POPIA;
3. the identification and codification of documents and ensuring adequate protection and maintenance of accuracy of documents where required;
4. providing a set framework and unified policy regarding the methods and procedures for the retention and destruction of documents;
5. ensuring records that are no longer required or documents that are of no value are destroyed properly and in accordance with the data retention schedule of Annexure D; and
6. providing assistance to employees in understanding the requirements relating to the protection of personal information and the retention and destruction of documents.

B. Stakeholders

- All employees

C. Scope

The types of information that Access Bank South Africa may be required to handle include details of current, past and prospective employees and clients, suppliers, and others that Access Bank South Africa communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in POPIA and other regulations. POPIA imposes restrictions on how Access Bank South Africa may use that information.

POPIA applies to the automated or non-automated processing of personal information entered into a record in any form (provided that when the recorded personal information is processed by non-

automated means, it forms part of a filing system or is intended to form part thereof) by or for Access Bank South Africa.

Annexure B to this policy sets out a list of 'Do and Do Nots' under POPIA.

This policy does not form part of any employee's contract of employment and may be amended at any time.

The IO is responsible for ensuring compliance with POPIA and with this policy. That post is held by **Head: Business Intelligence Department, 011 634-4300, popiInformationofficersa@accessbankplc.com**

Any questions or concerns about the operation of this policy should be referred in the first instance to the IO. See Annexure C for the IO appointment letter template.

If you consider that the policy has not been followed in respect of personal information about yourself or others, you should raise the matter with your line manager or the IO.

D. Objectives

This policy sets out Access Bank South Africa rules on personal information protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

E. Policy Statement

Everyone has rights with regard to how their personal information is handled. During the course of its activities Access Bank South Africa will collect, store and process personal information about Access Bank South Africa staff, customers, suppliers and other third parties. Access Bank South Africa recognises the need to treat it in an appropriate and lawful manner.

1. **PROCESSING CONDITIONS**

1.1. Anyone processing personal information must comply with the following eight processing conditions:

1. Condition 1: Accountability;
2. Condition 2: Processing Limitation;
3. Condition 3: Purpose Specification;
4. Condition 4: Further Processing Limitation;

5. Condition 5: Information Quality;

6. Condition 6: Openness;

7. Condition 7: Security Safeguards; and

8. Condition 8: Data Subject Participation.

1.2. ***Condition 1: Accountability***

1. Access Bank South Africa must ensure that the processing conditions are complied with.[1]

2. Access Bank South Africa has appointed an IO to encourage and support overall compliance with POPIA.

3. The IO is responsible for drafting an information security policy, which will, among other things, address document retention, access to information and classification of data.

4. Access Bank South Africa will furthermore designate specific individuals to monitor compliance with information security standards within each business area.

5. Training or awareness sessions for employees on information security will be conducted on a regular basis.

6. The Data Privacy Compliance Framework will assist in tracking the progress on compliance within the organisation (attached hereto as Annexure E).

1.3. ***Condition 2: Processing limitation***

1. Personal information may only be processed lawfully and in a manner that does not infringe on the privacy of a data subject.[2]

2. Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.[3]

[1] See section 6 of POPIA.
2 See section 9 of POPIA
3 See section 10 of POPIA.

3. There are a number of grounds that Access Bank South Africa may use in order to process personal information, please consult the IO when you collect any new type of personal information.

4. It is advisable to obtain voluntary, informed and specific consent from data subjects, where possible, before collecting their personal information. (See the model consent clause in Annexure F. Alternatively Access Bank South Africa may wish to obtain consent through the implementation of a Privacy Policy/External Privacy Statement.)

5. A data subject may withdraw consent at any time and such withdrawal of consent should be noted. A data subject may also object at any time on reasonable grounds, to the processing of its personal information, save if other legislation provides for such processing. Access Bank South Africa may then no longer process the personal information, unless it has another lawful justification for doing so.

6. Generally, personal information must be collected from the data subject directly except in certain circumstances which may include if the data subject has made personal information public or if collection from another source is necessary.[4]

1.4. ***Condition 3: Purpose specification***

1. Personal information may only be collected for specific, explicitly defined and lawful reasons relating to the functions or activities of Access Bank South Africa, of which the data subject is made aware.[5]

2. Personal information will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any personal information which is not necessary for that purpose will not be collected in the first place.

3. Once collected, personal information will only be processed for the specific purposes notified to the data subject when the personal information was first collected or for any other purposes specifically permitted by POPIA. This means that personal information will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the personal information is

[4] See section 12 of POPIA.
[5] See section 13 of POPIA.

processed, the data subject will be informed of the new purpose before any processing occurs.

4. Records of personal information may only be kept for as long as necessary for achieving the purpose for which the information was collected or subsequently processed, unless:[6]

- retention of the record is required or authorised by law;
- the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
- retention of the record is required by a contract between the parties thereto; or
- the data subject or a competent person where the data subject is a child has consented to the retention of the record.

5. Personal information will therefore not be kept longer than is necessary for the purpose for which it was collected. This means that personal information must be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form or be de-identified as soon as reasonably practicable after Access Bank South Africa is no longer authorised to retain the record. For guidance on how long certain personal information is likely to be kept before being destroyed, contact the IO or see the Document Retention Policy set out in Annexure D.

1.5. ***Condition 4: Further processing limitation***

1. Further processing of personal information must be compatible with purpose of collection, unless the data subject has consented to such further processing.[7]

2. Where personal information is transferred to a third party for further processing, the further processing must be compatible with the purpose for which it was initially collected, unless the data subject has consented to such further processing or it is permitted in terms of POPIA.

[6] See section 14 of POPIA.
[7] See section 15 of POPIA.

3. If personal information is to be used for any other purpose the further consent of the data subject must be obtained. Where this is not possible, the IO should be consulted.

4. Personal information may only be disclosed to other recipients in accordance with the provisions of the Personal Information Sharing Policy attached as Annexure G.

1.6. ***Condition 5: Information quality***

1. Access Bank South Africa must take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary in light of the purpose for which such information is collected.[8]

2. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information will be destroyed.

3. The IO will develop processes for:

- checking the accuracy and completeness of records containing personal information;
- dealing with complaints relating to the timeliness and accuracy of personal information;
- individuals to periodically verify and update their personal information;
- making individuals aware of these processes; and
- monitoring and tracking updates to personal information.

4. The IO will furthermore put procedures in place to verify that records containing personal information remain relevant, accurate and up-to-date.

1.7. ***Condition 6: Openness***

[8] See section 16 of POPIA.

1. Access Bank South Africa must take reasonably practicable steps to ensure that the data subject is aware of[9]:

   - the information being collected and where the information is not collected from the data subject, the source from which it is collected;
   - the name and address of Access Bank South Africa;
   - the purpose for which the information is being collected;
   - whether or not the supply of the information by that data subject is voluntary or mandatory;
   - the consequences of failure to provide the information;
   - any particular law authorising or requiring the collection of the information;
   - where applicable, the fact that the responsible party intends to transfer the information to a country or international organisation and the level of protection afforded to the information by that country or international organisation;
   - any further information such as the recipient or category of recipients of the information, the nature or category of the information and the existence of the right of access to and the right to rectify the information collected;
   - the existence of the right to object to the processing of personal information; and
   - the right to lodge a complaint to the Regulator and the contact details of the Regulator,

2. which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

3. By law all organisations in South Africa are required to have a PAIA manual which will outline to the public:

[9] See section 18 of POPIA.

- categories of personal information collected by Access Bank South Africa;
- purpose of processing personal information Access Bank South Africa;
- description of the categories of data subjects and of the information or categories of information relating thereto;
- the recipients or categories of recipients to whom the personal information may be supplied;
- planned transborder flows of personal information; and
- a general description of information security measures to be implemented by Access Bank South Africa.
- A PAIA manual template is attached as Annexure H.
- Access Bank South Africa processes personal information of its clients/customers, an external privacy statement is useful in providing data subjects with the requisite information in order for Access Bank South Africa to comply with this condition. (Our External Privacy Statement is attached as Annexure I and must also be published on Access Bank South Africa's website).
- The use of cookies on Access Bank South Africa's website requires that data subjects are aware of what cookies are active on the website, what user data they track, for what purpose, and where in the world this data is sent. Access Bank South Africa will notify data subjects by of these matters by means of a Cookie Policy (attached hereto as Annexure J.)
- For staff an Internal Privacy Notice describes how Access Bank South Africa will collect and use personal information about its staff during and after its working relationship with them, in accordance with the requirements of this condition should be implemented (attached hereto as Annexure K.)

1.8. ***Condition 7: Security safeguards***

1. Access Bank South Africa will keep all personal information secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure and conduct regular risk assessments to identify and manage all reasonably foreseeable internal and external risks to personal information under its control.

2. Access Bank South Africa will secure the integrity of the personal information under Access Bank South Africa control. (Common internationally recognised standards and/or practices that could be adopted include the ISO 27000 series (Information Security Management Standards), CoBIT (Control Objectives for Information Technology), ITIL (Information Technology Infrastructure Library) and PCI-DSS (Payment Card Industry Data Security Standard)).

3. In order to protect personal information Access Bank South Africa has implemented the following policies:

- Password Policy (attached hereto as Annexure L); and
- Bring Your Own Device Policy (attached hereto as Annexure M).
- Information Security Policy

Duty in Respect of Operators

1.9. Operators (i.e. third parties which may further process personal information collected by Access Bank South Africa) include call centres, outsourced payroll administrators, marketing database companies, recruitment agencies, psychometric assessment centres, document management warehouses, external consultants, credit bureaus and persons who clear the payment instructions of Access Bank South Africa's clients.

1. Access Bank South Africa will implement the following key obligations in respect of operators:

2. The operator may not process personal information on behalf of Access Bank South Africa without the knowledge and authorisation of Access Bank South Africa;

3. Access Bank South Africa will ensure that the operator implements the security measures required in terms of Condition 7: Security Safeguards;

4. There will be a written contract in place between Access Bank South Africa and the operator which requires the operator to maintain the confidentiality and integrity of personal information processed on behalf of Access Bank South Africa;

5. The written contract between Access Bank South Africa and the operator will include the provisions (with the necessary changes to detail) set out in Annexure N hereto; and

6. If the third party is located outside of South Africa, Access Bank South Africa will consult the IO. (Refer to chapter on transborder data transfers)

Capturing of Images and Use of Close Circuit Television

1.10. The use of photographs will comply with the Photography Policy (attached hereto as Annexure P). In addition, the use of any Closed Circuit Television (CCTV) to monitor and record activities for the purposes of safety and security will comply with the provisions of the CCTV Monitoring Policy (attached hereto as Annexure I.)

Duties in Respect of Security Compromises

1.11. In the event that personal information has been compromised, or if there is a reasonable belief that a compromise has occurred, Access Bank South Africa (or an operator processing personal information on its behalf) will comply with the Security Compromises Policy (attached hereto as Annexure R.)

1.12. Condition 8: Data subject participation

Request for Information

1.13. Access Bank South Africa recognises that a data subject has the right to request Access Bank South Africa to confirm, free of charge, whether or not it holds personal information about the data subject and request Access Bank South Africa to provide a record or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information at a prescribed fee.[10]

[10] See section 23 of POPI.

1.14. All users will comply with Access Bank South Africa's Subject Access Request Policy attached hereto as Annexure Q in respect of any access to personal information requests by data subjects.

Request to Correct or Delete

1.15. The data subject may request Access Bank South Africa IO to:

1. correct or delete personal information relating to the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, misleading or obtained unlawfully; or

2. destroy or delete a record of personal information about the data subject that Access Bank South Africa is no longer authorised to retain.

1.16. Access Bank South Africa will provide credible proof to the individual of the action that has been taken in response to the request.

1.17. If any changes to the personal information will have an impact on any decisions to be made about the individual, Access Bank South Africa will inform all third parties to whom the information has been disclosed, including any credit bureaus, of such changes.

2. FAIR AND LAWFUL PROCESSING

2.1. POPIA is intended not to prevent the processing of personal information, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

2.2. For personal information to be processed lawfully, certain requirements have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. In most cases when special personal information is being processed, the data subject's explicit consent to the processing of such information will be required.

2.3. Personal information about users may be processed for legal, personnel, administrative and management purposes and to enable the responsible party (i.e. Access Bank South Africa) to meet its legal obligations as an employer, for example to pay users, monitor their performance and to confer benefits in connection with their employment. Examples of when special personal information of users is likely to be processed are set out below:

1. information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

2. the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with employment equity legislation; and

3. in order to comply with legal requirements and obligations to third parties.

2.4. Personal information about customers, suppliers and other third parties may be processed. This includes cross-border transfers to other countries and international organisations, and the level of protection afforded to the information by that country or international organisation, including the processing of personal information on www.southafrica.accessbankplc.com; further processing by third parties, including the fact that members of the Group may access information on www.southafrica.accessbankplc.com; direct marketing; fraud prevention; SARB and SARS reporting and the like if applicable; and the recipient or category of recipients of the information

3. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

3.1. Personal information will be processed in line with data subjects' rights. Data subjects have a right to:

1. request access to any personal information held about them by Access Bank South Africa;

2. prevent the processing of their personal information for direct-marketing purposes;

3. ask to have inaccurate personal information amended; and

4. object to any decision that significantly affects them being taken solely by a computer or other automated process.

4. PROVIDING INFORMATION TO THIRD PARTIES

4.1. Users dealing with enquiries from third parties should be careful about disclosing any personal information held by Access Bank South Africa. In particular, they should:

1. check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

2. suggest that the third party puts their request in writing so the third party's identity and entitlement to the information may be verified;

3. refer to the IO for assistance in difficult situations; and

4. where providing information to a third party, do so in accordance with the eight processing conditions.

Annexure A PRIVACY IMPACT ASSESSMENT (POPIA AUDIT)

ACCESS BANK SOUTH AFRICA LIMITED AND ALL ITS SUBSIDIARIES AND BUSINESS AREAS

PROTECTION OF PERSONAL INFORMATION ACT

PRIVACY IMPACT ASSESSMENT

PLEASE READ THE FOLLOWING GUIDANCE NOTES BEFORE COMPLETING THIS FORM:

- The Protection of Personal Information Act 4 of 2013 (POPIA) was signed into law by the President on 19 November 2013. As an employee of Access Bank South Africa you are well aware that we have always been committed to quality and compliance with industry standards and applicable laws. POPIA exposes Access Bank South Africa and, indeed, all parties who process personal information of data subjects to potential liability.

- The purpose of this questionnaire is to find out what personal information Access Bank South Africa / your department collects or what personal information will be collected for a specific project and how that information is used to enable Access Bank South Africa to set standards for compliance with POPIA.

- Please complete this form in full and do not leave any blanks.

Name	
Position	

1 Step 1: Identify the need for a privacy impact assessment

Explain broadly what your department does or what a specific project aims to achieve.

2 Step 2: Identify the types of personal information processed and the types of processing

Do you use any of the following types of personal information?						
Type of information	**Yes/No**	**Does this information relate to children under the age of 18? If so, do you obtain parental/guardian consent?**	**Why do you use this information and what do you do with it? Is it linked to other personal information?**	**How long do you keep personal information where do you keep physical and electronic documents containing personal information (for example in a pigeon hole, in files that anyone can access, locked, in an electronic document management system etc.), how do you keep it secure and how do you destroy it?**	**How do you keep the information accurate and up to date?**	**Do you share this information with others or do others have access to such information? If so, with whom, how and why?**
information relating to the gender, sex, pregnancy, marital status, national, social origin, colour, sexual orientation, age, well-being, disability, conscience, culture, language and birth of the person						
information relating to the education or the medical, financial, criminal or						

employment history of the person						
any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person						
the personal opinions, views or preferences of the person						
correspondence sent by the person that is private or confidential nature						
the views or opinions of another individual about the person						
the name of the person						
Do you process any of the following types of special personal information?						
the religious or philosophical beliefs, race or ethnic origin, trade union						

membership, political persuasion, physical or mental health or sex life or biometric information (including fingerprints, voice recordings and images) of a person						

3 Step 3: Identify the use of personal information for direct marketing

Do you approach others, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply any goods or services to them or to request them to make a donation of any kind for any reason? If so, where do you obtain their contact details from and do you obtain consent (i.e. do they opt in) and do you allow them to opt out?

4 Step 4: Identify transborder transfers of personal information

Do you transfer personal information to other countries? If so, what types of personal information, to which countries and for what reason?

5 Step 5: Identify the justification for processing

Do you obtain consent from the relevant person before you process the personal information? If not, why do you think you should be allowed to use the information?

6 Step 6: Identify and assess risks

Describe the risks involved with the use of the personal information. (For example, does it have a negative impact on the privacy of others? Is there a risk of unauthorized access to the personal information (i.e. a data protection breach)?)

7 Step 7: Identify measures to reduce risk

What can you / our company do to reduce the risk identified above?

8 Step 8: Information Officer assessment

Information Officer to summarise privacy impact and measures to reduce risk

Annexure B POPIA - "DO AND DO NOTS"

1. **DO**

1.1. DO conduct an information retention audit by creating a matrix which clearly identifies the various categories of personal information held by each department of Access Bank South Africa, including emails, and setting out a precise retention policy for each category. (The POPIA Audit Questionnaire in Annexure A should be used for this purpose.)

1.2. DO designate someone as an IO and ensure this person is adequately trained and registered with the Regulator.

1.3. DO, where possible, obtain "voluntary, specific and informed" consent from a data subject, including customers of Access Bank South Africa, prior to processing his information, including his name, race, gender, marital status, address, identity number, e-mail address, physical address, and telephone number.

1.4. DO assume that Access Bank South Africa will probably only have one chance to obtain the prescribed consent.

1.5. DO ensure that obtains "optimum" consent.

1.6. DO remember that POPIA applies to paper files, information held electronically, video/DVD, audiotapes, photographs, images recorded on CCTV and other cameras, biometric information such as fingerprints etc.

1.7. DO be careful about sensitive data, namely data concerning race, political opinion, religious belief, trade union membership, physical or mental health, sex life, images and criminal offences.

1.8. DO ensure the integrity and safekeeping of personal information in Access Bank South Africa possession or under its control, by among other things, taking steps to prevent the information being lost, damaged, or unlawfully accessed.

1.9. DO define the purpose of gathering and processing of information, collect personal information only for a specific, explicitly defined and lawful purpose that is related to a function or activity of Access Bank South Africa, and hold personal information only when necessary.

1.10. DO process personal information in a lawful manner; personal information is processed lawfully when if it is adequate, relevant, and not excessive given the purpose for which it is processed.

1.11. DO take steps to notify the data subject that Access Bank South Africa holds personal information about him and tell him why Access Bank South Africa needs to do so.

1.12. DO check the rationale for any further processing and ensure further processing is compatible with the purpose for which the data was initially collected.

1.13. DO ensure that Access Bank South Africa has a written contract (data processing agreement) in place when sharing personal information with other organisations or third parties and that these parties enter into a Non-Disclosure Agreement.

1.14. DO ensure that personal information is entered into records accurately and that the information is complete, up to date, and not misleading.

1.15. DO obtain parental consent when collecting personal information about persons under the age of 18.

1.16. DO ensure that any paper record is properly filed or disposed of.

1.17. DO accommodate data subject requests, including requests to disclose the identity of all third parties that have had access to their information (which request Access Bank South Africa must attend to free of charge) and provide a record of personal information (which request Access Bank South Africa may attend to at a reasonable prescribed fee).

1.18. DO hold personal information in such a way that it can be collected for inspection at short notice.

1.19. DO direct any official requests to see personal information to the IO.

1.20. DO, as far as possible, de-identify (anonymise) personal information for statistical analysis.

1.21. DO respect the rights of a data subject, which include the right to confidentiality, which requires that Access Bank South Africa refuses requests from family, friends and employers for information about him, including references, unless the written consent of the data subject has been acquired.

1.22. DO retain records for required periods only as personal information must be destroyed, deleted, or “de-identified” as soon as the purpose for collecting the information has been achieved, unless it is a requirement of law to keep it for a longer period. A record of the information must be retained, however, if Access Bank South Africa has used it to make a decision about the data subject, including the CVs of prospective employees, for long enough for the data subject to request access to it. (Refer to the Document Retention Policy in Annexure D.)

1.23. DO review personal information kept in files, from time to time (at least annually) and dispose of unnecessary information as confidential waste.

1.24. DO consider providing “open references” for employees leaving Access Bank South Africa only (which are shown to the employee before they are sent to third parties).

1.25. DO, when writing documents, bear in mind that the data subjects have a right to see information relating to them.

1.26. DO note that transborder data transfer (including to neighbouring countries) is stringently regulated; therefore, seek further advice from the IO when this is to be done.

1.27. DO process personal information for the purpose of direct marketing by means of any form of electronic communication only if the data subject has given its consent in the prescribed form and manner to the processing or is a customer of Access Bank South Africa or is an existing customer.

1.28. DO process the personal information of a data subject who is a customer of Access Bank South Africa for direct marketing purposes only:

1.28.1. If Access Bank South Africa has obtained the contact details of the data subject in the context of the ‘sale’ of a service;

1.28.2. for the purpose of direct marketing of Access Bank South Africa own similar services; and

1.28.3. if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of its electronic details at the time when the information was collected and in each subsequent communication.

1.29. DO approach a data subject whose consent is required and who has not previously withheld such consent only once in order to request the consent of that data subject.

1.30. DO include in any communication for the purpose of direct marketing:

1.30.1. details of the identity of Access Bank South Africa; and

1.30.2. an address or other contact details to which the recipient may send a request that such communications cease (i.e. include an opt-out function).

1.31. DO make sure that any opt-outs are recorded appropriately.

1.32. DO take special care when accessing Access Bank South Africa computer network remotely and ensure that data is encrypted.

2. **DO NOTs**

2.1. DO NOT ignore POPIA. Ignorance may lead to a civil action for damages, regardless of whether intent or negligence can be proven on the part of Access Bank South Africa, and to an enforcement notice being issued by the Regulator (non-compliance with an enforcement notice is an offence).

2.2. DO NOT use old mailing lists.

2.3. DO NOT reveal personal information to third parties without the data subject's permission or justification.

2.4. DO NOT take up references without the consent of the data subject, i.e. only ever approach individuals named by the data subject.

2.5. DO NOT verify qualifications of employees or job seekers without the consent of the data subject.

2.6. DO NOT hold personal information about a person without explicit consent or advice from the IO.

2.7. DO NOT print personal information without a good reason.

2.8. DO NOT place personal information about an individual on the Internet without his/her permission, unless it is a condition of his/her employment.

2.9. DO NOT send personal information outside South Africa (including our neighbouring countries) without taking advice from the IO.

2.10. DO NOT leave personal information insecure in any way, whether it is physical files or information held electronically.

2.11. DO NOT allow staff to take personal information (such as credit checks) home without particular care for security.

2.12. DO NOT process personal information on a computer that is not owned or supplied by Access Bank South Africa.

2.13. DO NOT part with Access Bank South Africa computers without advice on deletion of data from the IO.

2.14. DO NOT use email for sending confidential communications or unencrypted personal information, as it is relatively insecure.

2.15. DO NOT use personal information held for one purpose for a different purpose without permission from the data subject.

2.16. DO NOT delete or alter any personal information after the IO has received a request to inspect and/or disclose that personal information.

2.17. DO NOT mention anything in email correspondence that Access Bank South Africa would not want a data subject to see; even deleted emails may be retrieved and revealed to those about whom they are written.

Annexure C IO APPOINTMENT LETTER TEMPLATE

[ON LETTERHEAD OF COMPANY]

PRIVATE AND CONFIDENTIAL
[INDIVIDUAL'S NAME]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [INDIVIDUAL'S NAME],

1. **Letter of appointment**

1.1. The board of directors (**Board**) of Access Bank South Africa Limited (**Company**) has appointed you as its Information Officer.

1.2. This letter sets out the main terms of your appointment. If you are unhappy with any of the terms, or need any more information, please let me know.

2. **Appointment**

2.1. Subject to the remaining provisions of this letter, your appointment shall be for an initial term of [**three months**] (Initial Term) commencing on [**DATE**] unless terminated earlier by either party giving to the other [one month's] prior written notice. After the Initial Term the Board will review your appointment.

2.2. Continuation of your appointment is contingent on your continued satisfactory performance and re-election by the Board and any relevant statutory provisions relating to the removal of an Information Officer.

2.3. Notwithstanding the above, the Company may terminate your appointment with immediate effect if, among other things, you have:

2.3.1. committed a material breach of your obligations under this letter;

2.3.2. committed any serious or repeated breach or non-observance of your obligations to the Company; and/or

2.3.3. been guilty of any fraud or dishonesty or acted in any manner which, in the Company's opinion, brings or is likely to bring you or the Company into disrepute or is materially adverse to the Company's interests.

3. **Role and Duties**

3.1. As Information Officer you will be responsible for ensuring compliance with the provisions of the Protection of Personal Information Act 4 of 2013 (POPIA) on behalf of the Company and your duties will include:

3.1.1. the encouragement of compliance, by the Company, with the conditions for the lawful processing of personal information set out in Chapter 3 of POPIA;

3.1.2. dealing with requests made to the Company pursuant to POPIA;

3.1.3. working with the Information Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA in relation to the Company;

3.1.4. communication with the Information Regulator, where necessary;

3.1.5. selecting, managing and acquiring resources (both hard copy and electronic) to meet the Company's current and anticipated needs;

3.1.6. classifying, collating and storing information, usually using special computer applications, for easy access and retrieval;

3.1.7. creating and searching databases;

3.1.8. cataloguing and indexing materials;

3.1.9. scanning and abstracting materials;

3.1.10. conducting information audits;

3.1.11. developing and managing electronic resources using, for example, online databases and content management systems;

3.1.12. writing and editing reports, publications and website content;

3.1.13. developing and managing internal information resources and networks via intranet sites;

3.1.14. overseeing the development of new information systems;

3.1.15. responding to data subject' requests using electronic and printed resources;

3.1.16. running effective enquiry and current awareness or 'alerting' services and developing communications strategies;

3.1.17. providing user education via leaflets, websites and tours of the library/information room;

3.1.18. publicising and marketing services, internally and externally, through publicity material, demonstrations, presentations and/or social media;

3.1.19. providing training and advice to colleagues and sometimes clients on the use of electronic information services;

3.1.20. managing a range of projects;

3.1.21. developing and exploiting multimedia information;

3.1.22. giving presentations and individual consultations.

3.1.23. supervising and training other information staff;

3.1.24. budget management;

3.1.25. developing, implementing, monitoring and maintaining a compliance framework;

3.1.26. conducting a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

3.1.27. developing, monitoring, maintaining and making available a manual as prescribed in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2002;

3.1.28. providing (upon request by any person) copies of the abovementioned manual to that person upon the payment of a fee to be determined by the Regulator from time to time;

3.1.29. developing internal measures together with adequate systems to process requests for information or access thereto; and

3.1.30. conducting internal awareness sessions regarding the provisions of POPIA, regulations made in terms of POPIA , codes of conduct, or information obtained from the Regulator.

3.2. Unless the Board specifically authorises you to do so, you shall not enter into any legal or other commitment or contract on behalf of the Company.

3.3. You shall be entitled to request all relevant information about the Company's affairs as is reasonably necessary to enable you to discharge your responsibilities as an Information Officer.

4. **Remuneration**

[COMPLETE IF APPLICABLE]

5. **Confidentiality**

5.1. You acknowledge that all information acquired during your appointment is confidential to the Company and should not be released, communicated or disclosed to third parties or used for any reason other than in the interests of the Company, either during your appointment or following termination (by whatever means), without prior clearance from the Board. This restriction shall cease to apply to any confidential information which may (other than by reason of your breach) become available to the public generally.

5.2. You acknowledge the need to hold and retain Company information (in whatever format you may receive it) under appropriately secure conditions.

5.3. Nothing in this paragraph 5 shall prevent you from disclosing information which you are entitled to disclose in terms of relevant legislation, provided that the disclosure is made in accordance with the provisions of such legislation and you have complied with the Company's policy from time to time in force regarding such disclosures.

6. **Induction**

After the commencement of your appointment, the Company will provide a comprehensive, formal and tailored induction. We will arrange for site visits and meetings with senior and middle management and the Company's auditors. You will be expected to make yourself available during the Initial Term for the purposes of the induction. The company secretary will contact you with further details.

7. **Training**

On an ongoing basis, and further to the annual evaluation process, the Company will arrange for you to develop and refresh your skills and knowledge in areas which are mutually identified as being likely to be required, or of benefit to you, in carrying out your duties effectively. You should try to make yourself available for any relevant training sessions which may be organised for the Board.

8. **Data protection**

8.1. By signing this letter you consent to the Company holding and processing personal information about you for legal, personnel, administrative and management purposes and in particular to the processing of any special personal information (as defined in POPIA) relating to you including, as appropriate:

8.1.1. information about your physical or mental health or condition in order to monitor sick leave and take decisions as to your fitness to perform your duties; or

8.1.2. your racial or ethnic origin or religious or similar beliefs in order to monitor compliance with equal opportunities legislation; or

8.1.3. information relating to any criminal proceedings in which you have been involved for insurance purposes and in order to comply with legal requirements and obligations to third parties; or

8.1.4. Any other special personal information to be processed, e.g Trade Union Membership, Political Opinions, Religious or Philosophical beliefs or sexual life.

8.2. You consent to the Company making such information available to [any of its group companies,] those who provide products or services to the Company [or any company in the Company's group] (such as advisers and payroll administrators), regulatory authorities, potential or future employers, governmental or quasi-governmental organisations and potential purchasers of the Company or the business in which you work.

8.3. You also consent to the transfer of such information to the Company's [or any group company's] business contacts outside South Africa in order to further [its OR their] business interests even where the country or territory in question does not maintain adequate data protection standards.

8.4. You shall comply with the Company's data protection policy, a copy of which is attached.

8.5. The Company may change its data protection policy at any time and will notify you in writing of any changes.

9. **Entire agreement**

9.1. This letter [and any document referred to in it] constitutes the entire terms and conditions of your appointment and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between you and the Company, whether written or oral, relating to its subject matter.

9.2. You agree that you shall have no remedies in respect of any representation, assurance or warranty (whether made innocently or negligently) that is not set out in this letter and you shall not have any claim for innocent or negligent misrepresentation based on any statement in this letter.

10. **Variation**

No variation of this letter shall be effective unless it is in writing and signed by you and the Company (or respective authorised representatives).

11. **Governing law and jurisdiction**

Your appointment with the Company and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of South Africa and you and the Company irrevocably agree that the courts of South Africa shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this appointment or its subject matter or formation (including non-contractual disputes or claims).

Please indicate your acceptance of these terms by signing and returning the attached copy of this letter to [NAME AND POSITION].

Yours sincerely

_____
For and on behalf of Access Bank South Africa
[POSITION]

I confirm and agree to the terms of my appointment as Information Officer of Access Bank South Africa as set out in this letter.
Signed on [DATE] by [NAME]

.....
[INFORMATION OFFICER'S SIGNATURE]

Annexure D DOCUMENT RETENTION POLICY

ACCESS BANK SOUTH AFRICA LIMITED

DOCUMENT RETENTION POLICY

1. **DEFINITIONS**

1.1. "**Destruction Authorities**" means permission granted by the Information Officer for the destruction of certain data, information or records, in whichever form;

1.2. "**IO**" means the information officer appointed in terms of PAIA and / or POPIA;

1.3. "**Non-Regulated Documents**" means documents, data, information or records that need to be retained for commercial purposes and so identified by Access Bank South Africa, fully detailed in Appendix B hereto;

1.4. "**PAIA**" means the Promotion of Access to Information Act 2 of 2000;

1.5. "**POPIA**" means the Protection of Personal Information Act 4 of 2013;

1.6. "**Regulated Document**" means all the documents, records and information detailed in Appendix A hereto;

1.7. "**Information, Communication, Technology Governance Committee**" means the committee body in Access Bank South Africa, who are responsible for creating a document retention policy and for its implementation;

1.8. "**Retention Schedule**" means the document setting out the retention periods for relevant data, information or records, as provided for in Record Retention Policy

1.9. "**User(s**)" means all employees employed by Access Bank South Africa and includes Access Bank South Africa directors, contract workers and the Retention Officer / Information Officer

2. **APPLICATION**

This Document Retention Policy should be read in conjunction with Access Bank South Africa Protection of Personal Information Policy and PAIA manual which, collectively, apply to all Users and, in certain circumstances, apply to suppliers and customers of Access Bank South Africa.

3. PURPOSE

The purpose of this policy is to supplement Access Bank South Africa's Protection of Personal Information Policy and the PAIA manual to ensure that Access Bank South Africa complies with document-retention provisions contained in applicable legislation ("regulatory compliance").

4. CREATION OF DOCUMENT MANAGEMENT ARCHIVE

4.1. As soon as reasonably possible after his/her appointment, the Information Officer shall ensure that an archive for Access Bank South Africa is constructed.

4.2. The archive may be:

4.2.1. In physical (i.e. paper) format.

4.2.2. In electronic format, provided that all the electronic records may only be stored onto the categories of storage medium prescribed by the Retention Committee and which meets the prescripts of the Retention Committee and Electronic Communications and Transactions Act 25 of 2002;

4.2.3. Outsourced to a third party service provider, provided all the requirements in terms of Access Bank South Africa's Record Retention Policy are met; and/or

4.2.4. A combination of the above.

4.3. Access Bank South Africa may decide to encompass the different ways of storing documents, depending on the type of document or record. It is advisable that the most cost-effective methods are used.

4.4. The legal requirements and aspects (not an extensive list) of electronic storage are highlighted in Appendix C attached to this policy.

5. MANAGEMENT OF REGULATED DOCUMENTS

5.1. All Regulated Documents (as detailed in Appendix A) that are created, received or handled by Users shall be forwarded to the Information Officer for archiving.

5.2. The Information Officer shall, upon receipt of the relevant Regulated Document, allocate an index number to the document and retain the document in the archive for the period detailed in Appendix A.

6. MANAGEMENT OF NON-REGULATED DOCUMENTS

6.1. All Non-Regulated Documents (as detailed in Appendix B) that are created, received or handled by Users shall be forwarded to the Information Officer for archiving.

6.2. The Information Officer shall, upon receipt of the relevant Non-Regulated Document, allocate an index number to the document and retain the document in the archive for the period detailed in Appendix B.

7. NAMING STANDARDS

7.1. The Information Officer shall inform all Users of the indexing standards and all Users shall apply such standards in the creation and classification of Access Bank South Africa documents.

7.2. The indexing standards should be objectively ascertainable from the face of the indexing standards document, and should not rely on the specific and personal knowledge of any one person, including the Information Officer, to be comprehensible.

8. USER DUTIES

8.1. Users shall not destroy documents or any form of data if such document or data falls in the categories detailed in Appendices A and B and without Destruction Authorities.

8.2. Documents falling within the categories of Appendices A and B shall be forwarded by hand or electronic mail to the Information Officer for retention.

9. E-MAIL DESTRUCTION

9.1. Users shall, on the last day of every month, delete all personal or non-Access Bank South Africa e-mail messages (incoming and outgoing as well as attachments thereto) from the User's e-mail programme. This is to as to avoid email congestion.

9.2. Users shall save and retain all e-mail messages (which have been assessed to determine whether it contains a record that needs to be retained as required by Access Bank South Africa's Record Retention Policy, in a folder and for a period as specified in the Retention Schedule.

10. DISPOSAL AND DESTRUCTION OF DOCUMENTS AND RECORDS

10.1. Documents or records that are not required to be kept in terms of either regulatory or non-regulatory prescriptions should be destroyed.

10.2. Regulatory Documents shall only be destroyed if the periods detailed in Appendix A have lapsed, subject to the approval of the Information Officer. Non-Regulatory Documents shall only be destroyed if the periods detailed in Appendix B have lapsed, subject to the approval of the Information Officer.

10.3. Duplicates and copies, when the originals are available and intact, should be destroyed.

10.4. Shredding of documents or records is the best option available for the destruction of such documents, especially confidential documents, whilst burning poses environmental and safety problems which will require additional safety and other measures to be complied with.

11. ELECTRONIC INFORMATION MANAGEMENT

Where the Information, Communication, Technology Governance Committee ('ITCGC') decides to manage and retain documents and records electronically, in whole or in part, the Information Officer shall see to the construction of an electronic archive that shall comply with and address the "retention", "original" and "evidence" requirements of the Electronic Communications and Transactions Act 25 of 2002 as detailed in Appendix C1 hereto and which shall be sufficiently secure.

12. PROTECTION OF PERSONAL INFORMATION

12.1. POPIA places an obligation upon Access Bank South Africa, as a responsible party, to collect, use and destroy personal information in a responsible and accountable way.

12.2. "Personal information" is broadly defined in POPIA to include a range of information relating to an identifiable, living, natural person, as well as an identifiable, existing juristic person, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity.

12.3. Access Bank South Africa will collect and store personal information for lawful purposes which are related to the functions and business activities of Access Bank South Africa, and such purposes will be compatible with and necessary in order to pursue and maintain the legitimate interests of Access Bank South Africa. Personal information may also be processed by Access Bank South Africa for the purposes of management, research, analysis, corporate reporting and improving business efficiencies.

12.4. Access Bank South Africa will take steps to ensure that its suppliers and customers are made aware of the specific purpose/s for which Access Bank South Africa collects and processes the personal information of a supplier or customer, and will furthermore destroy, delete or de-identify a record of the personal information of a supplier or customer as soon as reasonably practicable after Access Bank South Africa is no longer authorised to retain such record.

12.5. Access Bank South Africa will collect and store the personal information of Users, suppliers and customers in physical and/or electronic form, as the circumstances require.

12.6. Access Bank South Africa will always endeavour to secure the integrity and confidentiality of personal information which is in its possession or under its control.

12.7. Users and other data subjects have the right at any time to request that Access Bank South Africa confirms the personal information which it holds about Users, and to request that

Access Bank South Africa corrects any incorrect or inaccurate personal information which it holds about a User.

12.8. In accordance with POPIA, records of personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

12.8.1. Retention of the record is required or authorised by law;

12.8.2. Access Bank South Africa reasonably requires the record for lawful purposes related to its functions or activities;

12.8.3. Retention of the record is required by a contract between the parties thereto; or

12.8.4. The data subject or a competent person where the data subject is a child has consented to the retention of the record.

12.9. It is therefore important to consider the document-retention periods in the various statutes that may be applicable to Access Bank South Africa (see Appendix A). Please note that this list is not exhaustive and may be updated from time to time as required.

13. GENERAL REMARKS AND OFFENCES

13.1. It should be noted that once litigation commences, or where litigation is reasonably expected, all records which could reasonably become subject to discovery proceedings or relevant to the dispute must be retained. A court can draw negative inferences or impose penalties for improper destruction of records. Furthermore, if evidence relevant to litigation or pending litigation is destroyed it may constitute an obstruction of justice.

13.2. PAIA provides that where access to records is requested in terms of PAIA, a person who with the intent to deny such right, destroys, damages or alters a record; conceals a record; or falsifies a record; or makes a false record, commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding 2 (two) years. As a result, Access Bank South Africa will take steps to ensure that it always remains in compliance with its obligations under PAIA, and all other applicable law.

14. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Access Bank South Africa and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

15. **POLICY REVISION**

This policy has been reviewed by the IO, and is subject to change without prior notice.

CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Telephone number: 011 634-4300

APPENDIX A DOCUMENT RETENTION SCHEDULE

DOCUMENTS THAT SHOULD BE RETAINED IN TERMS OF LEGISLATION AND ACCEPTED INDUSTRY STANDARDS ("Legally Required Documents")

BASIC CONDITIONS OF EMPLOYMENT ACT 75 OF 1997 ("BCEA")	
APPLICATION AND GENERAL REMARKS	
The BCEA prescribes minimum employment conditions and standards for employees.	
DOCUMENT	**PERIOD OF RETENTION**
	ORIGINAL OR ELECTRONIC
1. Every employer must supply an employee, when the employee commences employment, in writing with the particulars set out in section 29.[11]	3 years from the date of the last entry in the record or after the termination of employment.
2. Every employer must keep a record containing at least the following information under the BCEA:[12] i. the employee's name and occupation; ii. the time worked by each employee; iii. remuneration paid to each employee; iv. the date of birth of any employee who is under the age of 18 (eighteen) years of age.	7 years.
3. In order to monitor or enforce compliance with an employment law, a labour inspector may—	

[11] Section 29 of the BCEA. See also section 33(1) which concerned information an employer must give an employee on each day the employee is paid.
[12] See section 31 of the BCEA.

i.	require a person to disclose information, either orally or in writing, and either alone or in the presence of witnesses, on any matter to which an employment law relates, and require that the disclosure be made under oath or affirmation;	
ii.	inspect, and question a person about, any record or document to which an employment law relates;	
iii.	copy any record or document referred to in section 66(b), or remove these to make copies or extracts;	
iv.	require a person to produce or deliver to a place specified by the labor inspector any record or document referred to in paragraph (b) of section 66 for inspection;	
v.	inspect, question a person about, and if necessary, remove, any article, substance or machinery present at a place referred to in section 65;	
vi.	inspect or question a person about any work performed; and	
vii.	perform any other prescribed function necessary for monitoring or enforcing compliance with an employment law	

COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT 130 OF 1993 ("COIDA")	
APPLICATION AND GENERAL REMARKS	
COIDA provides for compensation for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment, or for death sustained from these injuries at their place of work.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. The following documents should be retained:[13] i. Payrolls; ii. Accident books and records; iii. Salary revision schedules; iv. Staff records; v. Time and piecework records; vi. Wage and salary records (including overtime details). 2. The Director-General of the Department of Labour may subpoena any person who in his opinion is able to give information concerning the subject of any inquiry in terms of COIDA, or who is suspected to have or in the opinion of the Director-General has in his possession or custody or under his control any book, document or thing which has a bearing on the inquiry, to appear before him at a time and place specified in the	7 years.

[13] See section 81(2) of COIDA.

subpoena, to be interrogated or to produce such book, document or thing, and the Director-General may retain such book, document or thing for further investigation.[14] 3. A person authorized by the Director-General may— i. without previous notice, at all reasonable times enter any premises; ii. while he is on the premises, or at any time thereafter, question any person who is or was on the premises; iii. order any person who has control over or custody of any book, document or thing on or in those premises to produce to him forthwith, or at such time and place as may be determined by him, such book, document or thing; iv. at any time and place order any person who has the possession or custody of or is in the control of a book, document or thing relating to the business of an employer or previous employer, to produce forthwith or at such time and place as may be determined by him, such book, document or thing; v. seize any book, document or thing which in his opinion may serve as evidence in any matter in terms of this Act; vi. examine or cause to be examined any book, document or thing produced to him or seized by him, and make extracts therefrom or copies thereof, and order any person who in his opinion is qualified thereto to explain any entry therein; vii. order an employee to appear before him at such	

[14] Section 6 of COIDA. See also section 40 of COIDA which deals with the powers of the Director-General after having received notice of an accident.

time and place as may be determined by him, and question that employee.	

Occupational Health and Safety Act, No 85 of 1993 ("OHSA")	
APPLICATION AND GENERAL REMARKS	
OHSA provides for the health and safety of employees at work.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. An employer or user shall keep at a workplace or section of a workplace, as the case may be, a record in the form of Annexure 1, which record shall be open for inspection by an inspector, of all incidents which he or she is required to report in terms of section 24 of the Act and also of any other incident which resulted in the person concerned having had to receive medical treatment other than first aid.	3 years
2. A health and safety committee shall keep record of each recommendation made to an employer in terms of issues affecting the health of employees and of any report made to an inspector as contemplated in section 20(2) of the Act	3 years
3. Records of assessments and air monitoring, and the asbestos inventory.	Min of 40 years
4. Medical surveillance records.	Min of 40 years
5. Records of risk assessments and air monitoring results	Min of 40 years
6. Medical surveillance records	Min of 40 years

7. Records of assessments and air monitoring	30 Years
8. Medical surveillance records	30 Years
9. Records of assessments and air monitoring audiogram of every employee	Min of 40 years
10. Medical surveillance records	Min of 40 years
11. All records of assessments and noise monitoring	Min of 40 years
12. All medical surveillance records, including the baseline audiogram of every employee	Min of 40 years

THE COMPANIES ACT 71 OF 2008 ("Companies Act")	
APPLICATION AND GENERAL REMARKS	
The Companies Act consolidates the law that regulates all companies operating in South Africa. Records, when used with respect to any information pertaining to a company, are classified in the Companies Act as any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act or any other public regulations.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC[15]**
1. Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of this Act or any other public regulation must be kept[16]	7 years, or any longer period of time specified in any other applicable public regulation
2. A copy of the Memorandum of Incorporation and the rules of the company.	Life of the company.
3. A profit company must also maintain a securities register, or its equivalent as prescribed in the Act.	Life of the company.
4. Every public company that appoints a company secretary, auditor and audit committee has to maintain a record of its company secretaries and auditors. If this person is an individual, then the person's name and former name if applicable and his or her date of appointment must be recorded. Where a firm or juristic person is appointed, the name, registration number and registered office address of that firm or juristic person as well as the name of the individual determined by that firm per section 44(1) of the Auditing Profession Act 26 of 2005 to be	No timeframe provided in relation to the retention of these records and it is generally assumed that it should be kept for the life of the company.

[15] Section 24 of the Companies Act provides that records should be kept in a written, or other form, or manner, that allows that information to be converted into written form within a reasonable time.

[16] Section 24 of the Companies Act

responsible for performing the functions of auditor, must be recorded. Any changes in these particulars must be recorded as they occur, with the date and nature of such change.[17]	
5. Record of current and past directors, including, in respect of each director: i. full name and former names (if any); ii. identity number, or, if the person does not have one, his or her date of birth; iii. nationality and passport number, if the person is not South African; iv. occupation; v. date of his or her most recent election or appointment as director of the company; vi. the name and registration number of every other company or foreign company of which the person is a director and in the case of a foreign company, the nationality of that company.	7 years after the past directors have retired from the company.
6. Copies of all reports presented at an annual general meeting of the company.	7 years after the event or meeting occurred.
7. Copies of all annual financial statements required by the Companies Act.	7 years after the date on which each such particular statements were issued
8. Copies of all accounting records required by the Companies Act, for the current financial year and for the previous seven completed financial years of the company	for the previous 7 completed financial years of the company
9. Notice and minutes of all shareholders' meetings, including all resolutions adopted by them and any document that was made	7 years after the date each such resolution was adopted.

[17] See section 26 of the Companies Act.

available by the company to the holders of securities in relation to such resolution.	
10. Copies of all written communications sent generally by the company to all holders of any class of the company's securities.	7 years after the date on which such communication was issued.
11. Minutes of all meetings and resolutions of directors or directors' committees or the audit committee.	7 years after the date of each such meeting during which such resolution was adopted.

FINANCIAL INTELLIGENCE CENTRE ACT 38 OF 2001 ("FICA")	
APPLICATION AND GENERAL REMARKS	
FICA is aimed at preventing money laundering.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC[18]**
1. When an accountable institution is required to obtain information pertaining to a client or prospective client pursuant the institution must keep a record of that information. [19]	For at least five years from the date on which the business relationship is terminated.
2. An accountable institution must keep a record of every transaction, whether the transaction is a single transaction or concluded in the course of a business relationship which that accountable institution has with the client, that are reasonably necessary to enable that transaction to be readily reconstructed.[20]	For at least five years from the date on which that transaction is concluded
3. A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or ought reasonably to have known that- a) the business has received or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;	

[18] Electronic record keeping is expressly allowed - See section 22(2) of FICA read with section 16 of the Electronic Communications and Transactions Act 25 of 2002.
[19] Section 23 (a) of FICA
[20] Section 23 (b) of FICA

b) a transaction or series of transactions to which the business is a party – i. facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities; ii. has no apparent business or lawful purpose; iii. is conducted for the purpose of avoiding giving rise to a reporting duty under this Act; iv. may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service; or v. relates to an offence relating to the financing of terrorist and related activities; c) the business has been used or is about to be used in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities, must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Financial Intelligence Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.[21]	For at least five years from the date on which the report was submitted to the Centre

[21] Section 23 (c) of FICA

PRESCRIPTION ACT 68 OF 1969 ("Prescription Act")	
APPLICATION AND GENERAL REMARKS	
The Prescription Act consolidates and amends the laws relating to prescription.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
It is advisable, but not mandatory, to retain bills of exchange.[22]	6 years.

[22] See section 11(C) of the Prescription Act – the debt in relation to a bill of exchange prescribes after 6 years.

TAX ADMINISTRATION ACT 28 OF 2011

("Tax Administration Act")

APPLICATION AND GENERAL REMARKS

The Tax Administration Act provides for the effective and efficient collection of tax, the alignment of the administration provisions of the tax Acts (including the Income Tax Act 58 of 1962 and the Value Added Tax Act 89 of 1991) and the consolidation of the provisions into one piece of legislation to the extent practically possible.

The requirements of the Tax Administration Act to keep records, books of account or documents for a tax period apply to a person who has submitted a return for the tax period; is required to submit a return for the tax period and has not submitted a return for the tax period; or is not required to submit a return but has, during the tax period, received income, has a capital gain or capital loss, or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.[23]

The records, books of account, and documents must be kept or retained in their original form in an orderly fashion and in a safe place; in the form, including electronic form, as may be prescribed by the Commissioner of Tax in a public notice; or in a form specifically authorised by a senior South African Revenue Services ("**SARS**") official.[24]

DOCUMENT[25]	**PERIOD OF RETENTION**
	ORIGINAL OR ELECTRONIC
1. In respect of each employee the employer shall keep a record showing: the amount of remuneration paid or due by him to the employee; - the amount of employees' tax deducted or withheld from the remuneration paid or due; - the income tax reference number of that employee; - any further prescribed information.[26]	5 years from the date of submission of the return evidencing payment.
2. A person must keep the records, books of account or documents	5 years from the date of the

[23] See section 29(2) of the Tax Administration Act.
[24] See section 30 of the Tax Administration Act.
[25] See section 29 of the Tax Administration Act.
26 Schedule 4 paragraph 14 (2) of the Income Tax Act.

that enable the person to observe the requirements of a tax Act; are specifically required under a tax Act or by the Commissioner of Tax by public notice; and enable SARS to be satisfied that the person has observed these requirements.	submission of the return or from the end of the relevant tax period, as the case may be.

VALUE-ADDED TAX ACT 89 OF 1991 ("VAT ACT")	
APPLICATION AND GENERAL REMARKS	
The VAT Act provides for the taxation of the supply of goods and services as well as the importation of goods and services.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. In addition to the records required under the Tax Administration Act the following documents should be retained by a VAT vendor:[27] i. A record of all goods and services supplied by or to the vendor showing the goods and services, the rate of tax applicable to the supply and the suppliers or their agents, in sufficient detail to enable the goods and services, the rate of tax, the suppliers or the agents to be readily identified by the Commissioner of Tax, and all invoices, tax invoices, credit notes, debit notes, Company statements, deposit slips, stock lists and paid cheques relating thereto; ii. A record of all importations of goods and documents relating thereto; iii. Documentary proof, as is acceptable to the Commissioner of Tax, substantiating the vendor's entitlement to a deduction at the time a return in respect of the deduction is furnished;	5 years (calculated from the date of the last entry or from the date of completion of the transaction).

[27] See section 55(1) of the VAT Act.

iv. The charts and codes of account, the accounting instruction manuals and the system and programme documentation which describe the accounting system used in each tax period in the supply of goods and services; v. Any debtor and creditor list required to be prepared where a vendor's basis of accounting is changed in accordance with the VAT Act;[28] vi. Any documentary proof required to be obtained and retained where a rate of zero per cent has been applied by any vendor.[29]	

[28] See section 15 (9) of the VAT Act.
[29] See section 11(3) of the VAT Act.

LABOUR RELATIONS ACT 66 OF 1995 ("LRA")	
APPLICATION AND GENERAL REMARKS	
The LRA governs the relations between employers, employees, registered trade unions and registered employers' organizations and provide a framework for collective bargaining between the parties. The Act further stipulates that various records should be retained for future reference.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. Registered trade unions and registered employers' organisations must preserve each of its books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, and auditor's reports, in an original or reproduced form.[30]	3 years from the end of the financial year to which they relate.
2. With each monthly remittance in terms of section 13, the employer must give the representative trade union[31]— i. a list of the names of every member from whose wages the employer has made the deductions that are included in the remittance; ii. details of the amounts deducted and remitted and the period to which the deductions relate; and iii. a copy of every notice of revocation.	Indefinitely.
3. An employer must disclose to a trade union representative all relevant information that will allow the trade union	3 years from the end of the financial year to which they relate.

[30] See section 98(4) of the LRA.
[31] Section 13(5) of the LRA.

representative to perform effectively the functions under this Act.[32]	
4. Every registered employers' organisation must keep: i. a list of their members; ii. the minutes of their meetings, in an original or reproduced form; and iii. the ballot papers.	3 years from the date of every ballot.
5. Employers must keep prescribed details regarding the following matters:[33] i. strikes, lockouts or protest action involving their employees; ii. records of each employee, specifying the nature of any disciplinary transgressions, the action taken by the employer and the reasons for such action.	3 years from the date of the event or end of the period to which they relate.
6. Every employer must keep the records that an employer is required to keep in compliance with an applicable collective agreement, and an arbitration award. An employer must submit those records in response to a demand made by a bargaining council, commissioner or any person whose functions in terms of the LRA include the resolution of disputes.[34]	3 years from the date of the event or end of the period to which they relate.

[32] Section 16(2) of the LRA. Section 21(1) of the LRA also provides that an employer must disclose to the commissioner any information and facilities that are reasonably necessary for the commissioner to determine the membership or support of the registered trade union and section 89 provides that an employer must disclose to the workplace forum all relevant information that will allow the workplace forum to engage effectively in consultation and joint decision making.

[33] See section 205 of the LRA.

THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 ("ECTA")	
APPLICATION AND GENERAL REMARKS	
1. ECTA regulates electronic communication and prohibits the abuse of information. The Act provides conditions for the electronic collection of personal information and also for the timeframe that this information must be retained. 2. All personal data that has become obsolete must be destroyed.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
3. The following information must be kept: 3.1. personal information and the specific purpose for which the data was collected must be retained (by the person who electronically requests, collects, collates, processes or stores the information); and 3.2. a record of any third party to whom the information was disclosed.	As long as such information is used and at least 1 year thereafter.

THE CONSUMER PROTECTION ACT 68 OF 2008 ("CPA")	
APPLICATION AND GENERAL REMARKS	
The CPA applies to the promotion of goods and services, the supply of goods and services in terms of a transaction and the goods and services themselves. Document retention requirements are prescribed in relation to promotional competitions.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. The promoter of a promotional competition must retain:[35] 1.1. full details of the promoter, including identity or registration numbers, as the case may be, addresses and contact numbers; 1.2. the rules of the promotional competition; 1.3. a copy of the offer to enter into a promotional competition; 1.4. the names and identity numbers of the persons responsible for conducting the promotional competition; 1.5. a full list of all the prizes offered in the promotional competition; 1.6. a representative selection of materials marketing the promotional competition or an electronic copy of such	3 years.

[35] See regulation 11 of GNR.293 of 1 April 2011: Regulations (Government Gazette No. 34180).

marketing materials; 1.7. a list of all instances when the promotional competition was marketed, including details on the dates, the medium used and places where the marketing took place; 1.8. the names and identity numbers of the persons responsible for conducting the selection of prize winners in the promotional competition; 1.9. an acknowledgment of receipt of the prize signed by the prize winner, or legal guardian where applicable, and his or her identity number, and the date of receipt of the prize, or proof by the promoter that the prize was sent by post or other electronic means to the winner using his or her provided details; 1.10. declarations made under oath or affirmation by the persons responsible for conducting the promotional competition that the prize winners were to their best knowledge not directors, members, partners, employees, agents or consultants of or any other person who directly or indirectly controls or is controlled by the promoter or marketing service providers in respect of the promotional competition, or the spouses, life partners, business partners or immediate family members; 1.11. the basis on which the prize winners were determined; 1.12. a summary describing the proceedings to determine the winners, including the names of the persons participating in determining the prize winners, the date and place where that determination took place and whether those proceedings were open to the general public;	

1.13. whether an independent person oversaw the determination of the prize winners, and his or her name and identity number; 1.14. the means by which the prize winners were announced and the frequency of such announcements; 1.15. a list of the names and identity numbers of the prize winners; 1.16. a list of the dates when the prizes were handed over or paid to the prize winners; 1.17. in the event that a prize winner could not be contacted, the steps taken by the promoter to contact the winner or otherwise inform the winner of his or her winning a prize; 1.18. in the event that a prize winner did not receive or accept his or her prize, the reason for his or her not so receiving or accepting the prize, and the steps taken by the promoter to hand over or pay the prize to that prize winner.	

THE FOLLOWING ACTS, IF APPLICABLE, IMPOSE INDIRECT REPORTING/DISCLOSURE OBLIGATIONS		
Employment Equity Act 55 of 1998	Section 18(1)	When a designated employer engages in consultation in terms of this Act the employer must disclose to the consulting parties all relevant information that will allow those parties to consult effectively.
	Section 26	An employer must establish and, for the prescribed period, maintain, records in relation to its workforce, its employment equity plan and any other records relevant to its compliance with this Act. The record should be kept for 5 years after expiry of employment equity plan.

Competition Act 89 of 1998	Section 49A Section 54	At any time during an investigation in terms of the Act, the Competition Commissioner may summon any person who is believed to be able to furnish any information on the subject of the investigation, or to have possession or control of any book, document or other object that has a bearing on that subject- (a) to appear before the Commissioner or a person authorised by the Commissioner, to be interrogated at a time and place specified in the summons; or (b) at a time and place specified in the summons, to deliver or produce to the Commissioner, or a person authorised by the Commissioner, any book, document or other object specified in the summons. The member of the Competition Tribunal presiding at the hearing may (a) direct or summon any person to appear at any specified time and place; (b) question any person under oath or affirmation; (c) summon or order any person i. to produce any book, document or item necessary for the purpose of the hearing; ii. to perform any other act in relation to this Act.
Promotion of Access to Information Act 2 of 2000	Section 50	A requester must be given access to any record of a private body if- (a) that record is required for the exercise or protection of any rights;

		(b) that person complies with the procedural requirements in this Act relating to a request for access to that record; and (c) access to that record is not refused in terms of any ground for refusal contemplated in PAIA. A request contemplated in subsection (1) includes a request for access to a record containing personal information about the requester or the person on whose behalf the request is made.
Unemployment Insurance Act 63 of 2001	Section 56	Every employer must, as soon as it commences activities as an employer provide information regarding its employees to the commissioner.
Labour Relations Act 66 of 1995	Section 189(3) Section 197B	When an employer contemplates dismissing one or more employees for reasons based on the employer's operational requirements, the employer must issue a written notice inviting the other consulting party to consult with it and disclose in writing all relevant information. An employer that is facing financial difficulties that may reasonably result in the winding-up or sequestration of the employer, must advise consulting parties and an employer that applies to be wound up or sequestrated must at the time of making application, provide consulting parties with a copy of the application.

NO STATUTORY GUIDANCE – STANDARD PRACTICE	PERIOD OF RETENTION*
DOCUMENT	**ORIGINAL OR ELECTRONIC****
The following documents should be retained:	
1. General contracts – indemnities and guarantees	5
2. Licensing agreements	5
3. Rental and hire purchase agreements	5
4. General legal correspondence	3
5. Accounting related correspondence	5
6. Negotiations	5
7. Unsuccessful job applications	1
8. Insurance claims and accident reports (after date of settlement)	3
9. Patent related agreements and records	5
10. Trademark related agreements and records	5
	10
	5

*** Periods are "years" unless indicated otherwise**

** **See requirements in Appendix C in respect of electronic records.**

APPENDIX B

DOCUMENTS THAT SHOULD BE RETAINED BY THE COMPANY

FOR COMMERCIAL PURPOSES ("Commercially Required Documents")

INFORMATION THAT SHOULD BE RETAINED FOR COMMERCIAL PURPOSES	**PERIOD OF RETENTION**
DOCUMENT	**ORIGINAL AND/OR ELECTRONIC RETENTION**
The following documents should be retained by Access Bank South Africa 1. List any additional documents in need	

APPENDIX C REQUIREMENTS FOR ELECTRONIC RECORDS MANAGEMENT

Where a law requires information to be retained, that requirement is met by retaining such information in electronic format, if -

- the information contained electronically is accessible so as to be usable for subsequent reference;
- the data in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- the origin and destination of that data and the date and time it was sent or received can be determined.

APPENDIX C1 REQUIREMENTS TO "RETAIN" DOCUMENTS IN ELECTRONIC FORMAT

SECTION 16 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if -

a) the information contained in the data message is accessible so as to be usable for subsequent reference;

b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

APPENDIX C2 REQUIREMENTS TO ARCHIVE "ORIGINAL" DOCUMENTS IN AN ELECTRONIC ARCHIVE

SECTION 14 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if -

a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity must be assessed -

a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

b) in the light of the purpose for which the information was generated; and

c) having regard to all other relevant circumstances.

APPENDIX C3 REQUIREMENTS TO ARCHIVE EVIDENCE IN ELECTRONIC FORMAT

SECTION 15 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence -

a) on the mere grounds that it is constituted by a data message; or

b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to -

a) the reliability of the manner in which the data message was generated, stored or communicated;

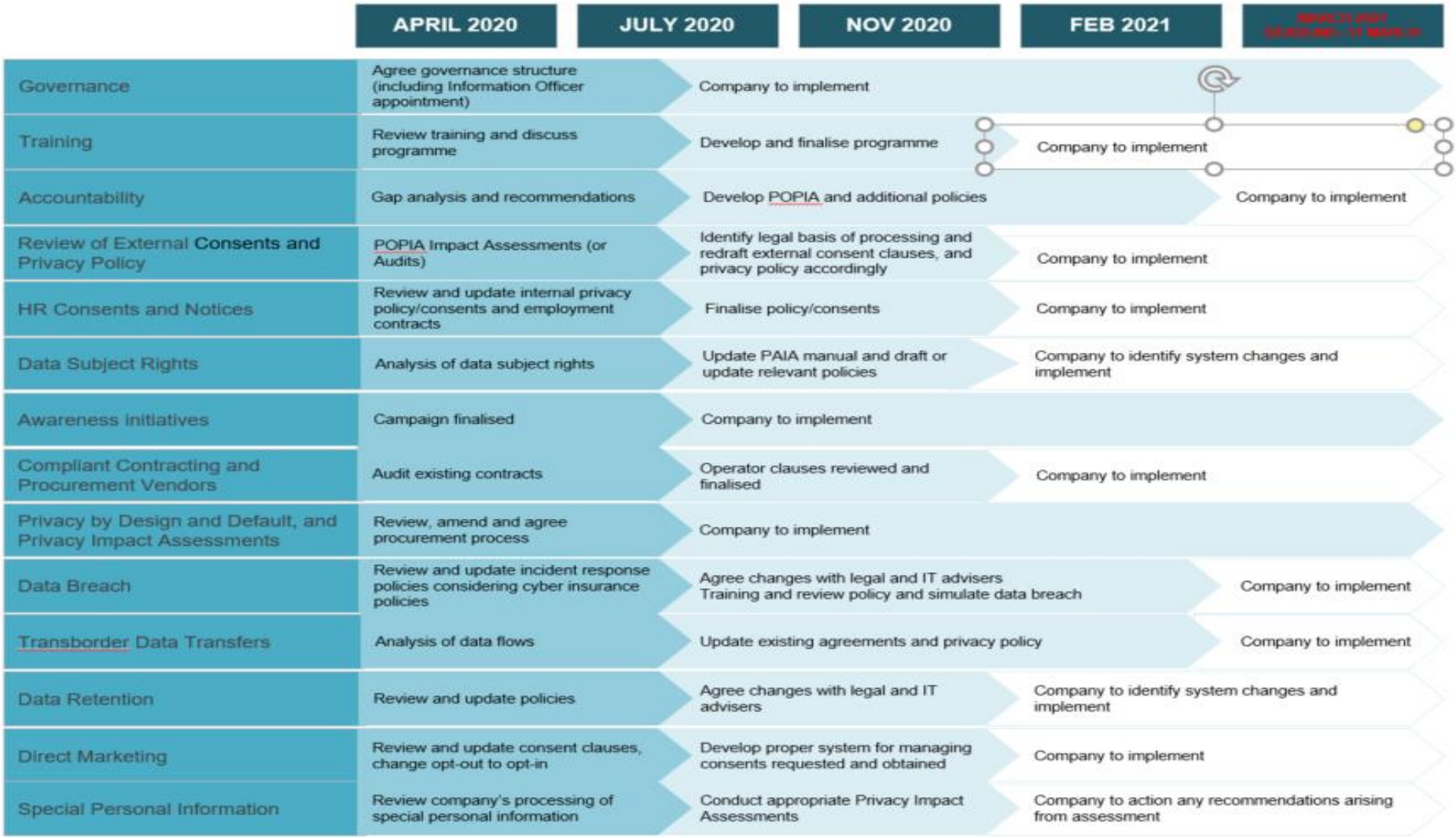
b) the reliability of the manner in which the integrity of the data message was maintained;

c) the manner in which its originator was identified; and

d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Annexure E PRIVACY COMPLIANCE FRAMEWORK



Annexure F MODEL POPIA CONSENT CLAUSE

Processing of Personal Information ***[This clause can also be replaced with a reference to the External Privacy Statement***

Please ensure that the name and address of Access Bank South Africa is stipulated on the agreement in compliance with section 18 of POPIA.]

The Client's privacy is very important to Access Bank South Africa and it will use reasonable efforts in order to ensure that any information, including personal information, provided by the Client, or which is collected from the Client, is stored in a secure manner.

The Client agrees to give (where applicable) honest, accurate and current information about the Client to Access Bank South Africa and to maintain and update such information when necessary.

The Client's personal information collected by Access Bank South Africa may be used for the following reasons:

Include cross-border transfers to other countries and international organisations, and the level of protection afforded to the information by that country or international organisation, including the processing of personal information on www.southafrica.accessbankplc.com further processing by third parties, including the fact that members of the Group may access information onwww.southafrica.accessbankplc.com; direct marketing; fraud prevention; SARB and SARS reporting and the like if applicable; and the recipient or category of recipients of the information.

The Client acknowledges that any information supplied to Access Bank South Africa in terms of these Terms of Business is provided voluntarily.

By submitting any information to Access Bank South Africa in any form the Client further acknowledges that such conduct constitutes an unconditional, specific and voluntary consent to the processing of such information by Access Bank South Africa under any applicable law in the manner contemplated above, which consent shall, in the absence of any written objection received from the Client, be indefinite and/or for the period otherwise required in terms of any applicable law.

Unless the Client has consented, Access Bank South Africa will not sell, exchange, transfer, rent or otherwise make available any personal information about the Client (such as name, address, email

address, telephone or fax number) to other parties and the Client indemnifies Access Bank South Africa from any unintentional disclosures of such information to unauthorized persons.

Should the Client believe that Access Bank South Africa has utilised the Client's personal information contrary to applicable law, the client shall first resolve any concerns with Access Bank South Africa. If the Client is not satisfied with such process, the Client has the right to lodge a complaint with the Information Regulator.

Annexure G **PERSONAL INFORMATION SHARING POLICY**

1. COMMITMENT

Access Bank South Africa takes the protection of personal information seriously and aims to comply with POPIA.

2. APPLICABILITY

2.1. This Personal Information Sharing Policy (the policy) applies to all staff working for Access Bank South Africa which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. This policy is in addition to other requirements which may be necessary for specific operations and it is your responsibility to familiarise yourself with this policy.

2.2. "Personal information" means any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. Personal information includes, for example, names and addresses, e-mail addresses, recruitment details, financial history and the like. It also includes opinions about individuals as well as facts and also applies to corporate contacts.

2.3. "Special personal information" is information such as religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.

3. OBLIGATIONS

3.1. Purpose definition and limitation

3.1.1. Personal information can only be collected and further processed for lawful, specific and explicitly defined purposes related to a function or activity of Access Bank South Africa.

3.1.2. You will find an indication of such purposes in Access Bank South Africa Protection of Personal Information Policy and website privacy policy.

3.1.3. After personal information has been collected by Access Bank South Africa it cannot be processed for purposes which are incompatible with the original ones.

3.1.4. For example, this means that personal information processed by the HR department for HR purposes will likely not be able to be lawfully processed by the marketing department for marketing purposes.

3.2. Personal information to be kept confidential

3.2.1. Access Bank South Africa must keep personal information confidential and safe from undue disclosures.

3.2.2. That means that sharing personal information with an external third party is an exception to the confidentiality rule, and must be analysed in detail to ensure lawfulness, notably considering:

3.2.2.1. Whether the purpose for which the external third party requires the personal information is compatible to the original purpose for which the information was collected;

3.2.2.2. Whether sharing the personal information with the external third party will constitute a transborder flow of information; and

3.2.2.3. Whether sharing the personal information with the external third party will likely put the information at risk due to the poor security measures the third party has in place.

4. PROCEDURES TO FOLLOW

4.1. If you receive a request for personal information you must: (a) notify the IO who will guide you or, as the case may be, lead the procedures; and follow the flowchart attached as Appendix A.

4.2. If you are required to share personal information, you must consider whether the personal information is to be shared internally (i.e. within Access Bank South Africa) or externally (i.e. with an agent, a public authority, an unconnected third party or other entities within Access Bank South Africa). When you are certain of the type of request you received, please check the flowchart for guidance on the specific steps to take.

4.3. If you are unsure which category the personal information sharing falls into, please contact the IO for further advice.

4.4. You should document at all times any questions asked, answers given and authorisation gained by any parties involved when dealing with a personal information sharing request.

4.5. Where you are asked to share personal information with unconnected third parties / public authorities, the IO will handle the process himself/herself.

5. CLIENT INFORMATION

Personal information relating to clients should not be shared with third parties, including other entities within the Access Bank South Africa group without seeking further guidance from the IO.

6. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Access Bank South Africa and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

7. POLICY REVISION

This policy has been reviewed by the IO, and is subject to change without prior notice.

8. CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Telephone number: 011 634-4300

Access Bank South Africa Limited

THE PROMOTION OF ACCESS TO INFORMATION MANUAL

("**Manual**")

INTRODUCTION

Access Bank South Africa Limited, previously known as Grobank Limited, ("the Bank", "we" or "us") was established in 1947 with the aim of servicing financial needs, supporting and backing commercial activities, to the entire local entrepreneurial business community, to accommodate the multilingual and socio-economic changes of South Africa.

The Bank possesses principal clearing bank status and is a fully authorised dealer in foreign exchange. It strives to become the preferred financial service provider in the market by supplying the appropriate financial solutions, nurturing a culture of personal service excellence and innovation through commitment and professionalism thereby exceeding the expectations of its clients.

The Bank is committed to endorse and support The Code of Banking Practice and its employees are guided by high ethical standards.

BACKGROUND TO PAIA AND POPIA

PAIA was enacted on 3 February 2000, giving effect to the Constitutional right of access to any information held by the State, and any information held by another person that is required for the exercise or protection of any right. Where a request is made in terms of PAIA, the public body to which the request is made is obliged to release the information, except where PAIA expressly provides that the information may or must not be released.

Where a request is made in terms of PAIA to a private body, that private body must disclose the information if the requester is able to show that the record is required for the exercise or protection of any rights, and provided that no grounds of refusal contained in PAIA are applicable. PAIA sets out the requisite procedural issues attached to information requests. In terms of Section 51 of PAIA, Access Bank South Africa is required to compile a Manual, which provides information as prescribed in PAIA.

POPIA, on the other hand, promotes the protection of personal information processed by public and private bodies, including certain conditions to establish minimum requirements for the processing of personal information. POPIA amends certain provisions of PAIA, balancing the need for access to information against the need to ensure the protection of personal information by providing for the establishment of an Information Regulator to exercise certain powers and perform certain duties and functions in terms of POPIA and PAIA, providing for the issuing of codes of conduct and providing for the rights of persons regarding unsolicited

electronic communications and automated decision making in order to regulate the flow of personal information and to provide for matters concerned therewith.

PURPOSE OF THE MANUAL

This manual is intended to foster a culture of transparency and accountability within the Financial Services Industry by giving effect to the right to information held by a private body that is required for the exercise or protection of any right, and actively promoting a society in which the people of South Africa have access to information to enable them to exercise and protect their rights.

Section 69 of PAIA, recognizes that justifiable limitations of the right to access may be permitted. Such justifiable limitations include but are not limited to:

- Reasonable protection of privacy;
- Commercial confidentiality
- Effective, efficient and good governance

The manual provides a generic format, which will enable requesters to obtain the records, which they are entitled to under PAIA in a quick and accessible manner.

PART 1

CONTACT DETAILS OF ACCESS BANK SOUTH AFRICA LIMITED

Name of Private Body: Access Bank South Africa Limited

Physical Address: Block 3, Inanda Greens Business Park, 54 Wierda Road West, Wierda Valley, Sandton, 2196, South Africa

Postal Address:	PO Box 784921, Sandton, 2146
Head of Body:	Mr Barend Johannes van Rooy
Information Officer:	Mr. Brendan van Zyl
Electronic Mail:	popiInformationofficersa@accessbankplc.com
Telephone Number:	+2711 634 4300
Fax:	+2711 836 2220

PART 2

A formal guide, as stipulated in Section 10, on how to use PAIA is available and can be obtained from the South African Human Rights Commission ("Commission") at the following address:

CONTACT DETAILS: SA HUMAN RIGHTS COMMISSION.

THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION: PAIA Unit

The Research and Documentation Department
Private Bag 2700
HOUGHTON
2041

Telephone Number:	(011) 484 8300
Fax Number:	(011) 484 0582
Website:	www.sahrc.org.za
Email:	paia@sahrc.org.za

INFORMATION REGULATOR AND GUIDE

The assigned powers of the Commission will, in future be transferred to the newly approved Information Regulator (established in terms of POPIA).

The Information Regulator will report directly to Parliament and will oversee and regulate all matters regarding POPIA and PAIA.

An official guide will be or has been compiled which contains information to assist a person wishing to exercise a right of access to information in terms of PAIA and POPIA. This guide will be made available by the Information Regulator. Copies of the updated guide are available from Information Regulator in the manner prescribed. The Information Regulator's contact details are set out below.

- Tel: 012 406 4818
- Fax: 086 500 3351
- Email: inforeg@justice.gov.za
- Website: http://www.justice.gov.za/inforeg/.

RECORDS HELD BY THE BANK

The Bank maintains records on the following categories and subject matters. However, please note that recording a category or subject matter in this Manual does not imply that a request for access to such records would be granted.

Records available in terms of legislation (Section 51(1)(d))

- Basic Conditions of Employment No. 75 of 1997
- Companies Act No. 71 of 2008
- Compensation for Occupational Injuries and Health Diseases Act No. 130 of 1993
- National Credit Act No. 34 of 2005, as amended
- Copyright Act No. 98 of 1978
- Consumer Protection Act No. 68 of 2008
- Currency and Exchanges Act No. 9 of 1933
- Employment Equity Act No. 55 of 1998
- Financial Advisory and Intermediary Services Act No. 37 of 2002
- Financial Intelligence Centre Act No. 38 of 2001
- Financial Services Board Act No. 97 of 1990
- Income Tax Act No. 95 of 1967
- Insolvency Act No. 24 of 1936
- Labour Relations Act No. 66 of 1995
- Occupational Health & Safety Act No. 85 of 1993
- SA Reserve Bank Act No. 90 of 1989
- Skills Development Levies Act No. 9 of 1999
- Skills Development Act No. 97 of 1998
- Stamp Duties Act No. 77 of 1968
- Unemployment Contributions Act No. 4 of 2002
- Unemployment Insurance Act No. 63 of 2001
- Value Added Tax Act No. 89 of 1991

PART 3

ACCESS TO THE RECORDS HELD BY ACCESS BANK SOUTH AFRICA

This clause serves as a reference to the records that Access Bank South Africa holds.

It should be noted however, that the accessibility of the documents listed below, may be subject to the specified grounds of refusal.

The information is classified and grouped according to records relating to personnel, clients and other party

PERSONNEL RECORDS

- Personal records provided by personnel;
- Records provided by a third party relating to personnel;
- Conditions of employment and other personnel-related contractual and quasi-legal records;
- Internal evaluation records and other internal records;
- Correspondence relating to personnel;
- Training schedules and material.

Personnel refer to any person who works for, or provides services to or on behalf of Access Bank South Africa, and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of Access Bank South Africa. This includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff, as well as contract workers.

CLIENT RELATED RECORDS

- Records provided by a client to a third party acting for or on behalf of Access Bank South Africa;
- Records provided by a third party;
- Records generated by or within Access Bank South Africa relating to its clients, including transactional records.

A *Client* refers to any natural or juristic entity that receives services from Access Bank South Africa.

OTHER PARTY RECORDS

Records held by Access Bank South Africa pertaining to other parties, including without limitation, financial records, correspondence, contractual records, records provided by the other

party, and records third parties have provided about the contractors/suppliers.

Access Bank South Africa may possess records pertaining to other parties, including without limitation contractors, suppliers, subsidiary / holding companies, agencies, joint venture companies and service providers. Alternatively, such other parties may possess records that can be said to belong to Access Bank South Africa.

RECORDS OF ACCESS BANK SOUTH AFRICA

This paragraph sets types of records Access Bank South Africa holds. The accessibility of these records (or information in these records), may be subject to the grounds of refusal set out below.

- Financial records
- Operational records
- Databases
- Information Technology
- Marketing records
- Internal correspondence
- Product Records
- Statutory records
- Internal Policies and Procedures
- Treasury related records
- Securities records
- Statutory limitations imposed by the Protection of Personal Information Act, 4 of 2013

These records include, but are not limited to, the records which pertain to Access Bank South Africa's own affairs and are confidential by nature.

GROUNDS FOR REFUSAL OF ACCESS TO RECORDS

The main grounds for Access Bank South Africa to refuse a request for information relates to the:

- Mandatory protection of the privacy of a third party who is a natural person, which would involve the unreasonable disclosure of personal information of that natural person;
- Mandatory protection of the commercial information of a third party, if the record contains:
    - Trade secrets of that third party;
    - Financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of that third party;

- Information disclosed in confidence by a third party to Access Bank South Africa, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;

- Mandatory protection of confidential information of third parties if it is protected in terms of any agreement;
- Mandatory protection of the safety of individuals and the protection of property;
- Mandatory protection of records which would be regarded as privileged in legal proceedings;
- The commercial activities of Access Bank South Africa, which may include:
  - Trade secrets of Access Bank South Africa
  - Financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interest of Access Bank South Africa;
  - Information which, if disclosed could put Access Bank South Africa at a disadvantage in negotiations or commercial competition;
  - A computer program which is owned by Access Bank South Africa and which is protected by copyright.
- The research information of Access Bank South Africa or a third party, if its disclosure would disclose the identity of Access Bank South Africa, the researcher or the subject matter of the research and would place the research at a disadvantage

Requests for information that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources shall be refused.

REMEDIES AVAILABLE WHEN ACCESS BANK SOUTH AFRICA REFUSES A REQUEST FOR INFORMATION

- INTERNAL REMEDIES
  - Access Bank South Africa does not have internal appeal procedures. As such, the decision made by the Information Officer is final, and requestors will have to exercise such external remedies at their disposal if the request for information is refused, and the requestor is not satisfied with the answer supplied by the Information Officer.
- EXTERNAL REMEDIES
  - A requestor that is dissatisfied with an Information Officer's refusal to disclose information may apply to a Court for relief within 30 days of notification of the decision.
  - Likewise, a third party dissatisfied with an information officer's decision to grant a

request for information, may within 30 days of the decision, apply to a Court for relief.

REQUEST PROCEDURE

- Form of request
    - The requester must comply with all the procedural requirements contained in PAIA relating to the request for access to a record
    - The requester must complete the prescribed form enclosed herewith Appendix 1 and submit it together with a payment of a request fee, if applicable to the Information Officer at the physical, postal address, fax number or electronic mail address as stated in point 4 above.
    - In the event of the request being made at branch level, the procedure stated herein shall apply with the exception that the request form will, together with all other necessary requirements be submitted to the Information Officer of Access Bank South Africa who will deal with the respective request.
    - The requester must provide sufficient detail on the request form to enable the Information Officer to identify the record and the requester.
    - The requester should indicate which form of access is required and should also indicate if any other manner is to be used to inform the requester and state the necessary particulars to be so informed.
    - The requester must state that he/she requires the information in order to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. In addition, the requester must clearly specify why the record is necessary to exercise or protect such a right.
    - If a request is made on behalf of another person, then the requester must submit proof of the capacity in which the requester is making the request to the reasonable satisfaction of the Information Officer. If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request verbally.
    - Access Bank South Africa will process the request within 30 days, unless the requestor has stated special reasons which would satisfy the Information Officer that circumstances dictate that the above time periods not be complied with.
    - The requester shall be informed whether access has been granted or denied. If in addition, the requester requires the reasons for the decision in any other manner, he/she must state the manner and the particulars so required.

FEES

- PAIA provides for two types of fees, namely:
    - A request fee, which will be a standard fee; and
    - An access fee, which must be calculated by taking into account reproduction costs, search and preparation time and cost, as well as postal costs.
    - When the request is received by the Information Officer, such officer shall by notice require the requester, other than a personal requester, to pay the prescribed request fee (if any), before further processing of the request.
- If the search for the record has been made and the preparation of the record for disclosure, including arrangement to make it available in the requested form, requires more than the hours prescribed in the regulations for this purpose, the information officer shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.
- The Information Officer shall withhold a record until the requester has paid the fees as indicated in Appendix 2
- A requester whose request for access to a record has been granted, must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure including making arrangements to make it available in the request form.
- If a deposit has been paid in respect of a request for access, which is refused, then the Information Officer concerned must repay the deposit to the requester.

DECISION

- The Bank will, within 30 days of receipt of the request, decide whether to grant or decline the request and give notice with reasons (if required) to that effect.
- The 30 day period with which Access Bank South Africa has to decide whether to grant or refuse the request, may be extended for a further period of not more than thirty days if the request is for a large number of information, or the request requires a search for information held at another office or division of Access Bank South Africa and the information cannot reasonably be obtained within the original 30 day period. The Bank will notify the requester in writing should an extension be sought.

PART 4

POPIA REQUIREMENTS PERTAINING TO THE PROCESSING OF PERSONAL INFORMATION

PURPOSE OF PROCESSING

- In terms of POPIA, data must be processed for a specified purpose. The purpose for which data is processed by the Bank will depend on the nature of the data and the particular data subject. This purpose is ordinarily disclosed, explicitly or implicitly, at the time the data is collected.
- In general, personal information is processed for purposes of onboarding clients and suppliers, service or product delivery, records management, security, employment and related matters.

ACCESS TO PERSONAL INFORMATION

- POPIA provides that a data subject may, upon proof of identity, request the Bank to confirm, free of charge, all the information it holds about the data subject and may request access to such information, including information about the identity of third parties who have or have had access to such information.
- POPIA also provides that where the data subject is required to pay a fee for services provided to him/her, the Bank must provide the data subject with a written estimate of the payable amount before providing the service and may require that the data subject pays a deposit for all or part of the fee.
- Grounds for refusal of the data subject's request are set out in PAIA and are discussed above.
- POPIA provides that a data subject may object, at any time, to the processing of personal information by the Bank, on reasonable grounds relating to his/her particular situation, unless legislation provides for such processing. The data subject must complete the prescribed form attached hereto as **Appendix 3** and submit it to the Information Officer at the postal or physical address, facsimile number or electronic mail address set out above.
- A data subject may also request the Bank to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or destroy or delete a record of personal information about the data subject that the Bank is no longer authorised to retain records in terms of POPIA's retention and restriction of records provisions.
- A data subject that wishes to request a correction or deletion of personal information or the destruction or deletion of a record of personal information must submit a request to the

Information Officer at the postal or physical address, facsimile number or electronic mail address set out above on the form attached hereto as **Appendix 4.**

CATEGORIES OF DATA SUBJECTS

The Bank holds information and records on the following categories of data subjects:

- Employees / personnel of the Bank;
- Clients of the Bank;
- Any third party with whom the Bank conducts its business services;
- Contractors of the Bank;
- Suppliers of the Bank.

(This list of categories of data subjects is non-exhaustive.)

THE CATEGORIES OF RECIPIENTS TO WHOM THE INFORMATION IS SUPPLIED

Depending on the nature of the data, the Bank may supply information or records to the following categories of recipients:

- Statutory oversight bodies, regulators or judicial commissions of enquiry making a request for data;
- Any court, administrative or judicial forum, arbitration, statutory commission, or ombudsman making a request for data or discovery in terms of the applicable rules (i.e. the Competition Commission in terms of the Competition Act 89 of 1998);
- South African Revenue Services, or another similar authority;
- Anyone making a successful application for access in terms of PAIA; and
- Subject to the provisions of POPIA and the National Credit Act No. 34 of 2005, the Bank may share information about a client's creditworthiness with any credit bureau or credit providers industry association or other association for an industry in which the Bank operates.

PLANNED TRANSBORDER FLOWS OF INFORMATION

If a data subject visits the Bank's websites from a country other than the country in the Bank's servers are located (currently in South Africa), the various communications will necessarily result in the transfer of information across international boundaries.

The Bank may need to transfer a data subject's information to other group companies or service providers in countries outside South Africa, in which case the Bank will fully comply with applicable data protection legislation. This may happen if the Bank's servers or suppliers and

service providers are based outside South Africa, or if the Bank's services are hosted in systems or servers outside South Africa and/or if a data subject uses the Bank's services and products while visiting countries outside this area. These countries may not have data-protection laws which are similar to those of South Africa.

SECURITY MEASURES IMPLEMENTED TO ENSURE THE CONFIDENTIALITY AND PRIVACY OF THE INFORMATION WHICH IS TO BE PROCESSED

The Bank is committed to implementing leading data security safeguards.

The Bank has specialised security teams who constantly review and improve the Bank's measures to protect data subject's personal information from unauthorised access, accidental loss, disclosure or destruction.

If the Bank has a contract with another organisation to provide it with services or a service on the Bank's behalf to process a data subject's personal information, the Bank will make sure it has appropriate security measures and only process the information in the way the Bank has authorised them to.

These organisations won't be entitled to use a data subject's personal information for their own purposes. If necessary, the Bank's security teams will check them to make sure they meet the security requirements the Bank has set.

Communications over the internet (such as emails) are not secure unless they have been encrypted. A data subject's communications may go through a number of countries before being delivered – as this is the nature of the internet. The Bank cannot accept responsibility for any unauthorised access or loss of personal information that is beyond the Bank's control.

AVAILABILITY OF THE MANUAL

This manual is available for inspection at the Head Office of Access Bank South Africa and can also be accessed from Access Bank South Africa website: www.southafrica.accessbankplc.com

APPENDIX 1

PRESCRIBED FORM TO BE COMPLETED BY A REQUESTER

FORM B: REQUEST FOR ACCESS TO RECORDS OF PRIVATE BODY

A. Particulars of Grobank Limited.

The Information Officer

Access Bank South Africa Limited

Building 3, Inanda Greens Business Park,

54 Wierda Road West,

Wierda Valley, Sandton

2196

P. O. Box 784921

Sandton

2146

Telephone: 011-634 4355

Fax: 011-836 2220

E-mail: PAIAsa@accessbankplc.com

B. Particulars of person requesting access to the record

a) The particulars of the person who requests access to the records must be recorded below
b) Furnish an address and/or fax number in the Republic to which information must be sent.
c) Proof of the capacity in which the request is made, if applicable, must be attached

Full Name and Surname: _____

Identity Number : _____

Postal Address : _____

Telephone Number : _____

Fax Number : _____

E-mail address : _____

Capacity in which request is made, when made on behalf of another person:

_____

C. Particulars of person of whose behalf request is made:

This section must be completed only if a request for information is made on behalf of another person

Full Name and Surname: _____

Identity Number : _____

D. Particulars of record:

a) *Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.* b) *If the provided space is inadequate, please continue on a separate folio and attach it to this form.* ***The requester must sign all the additional folios.***

1. Description of the record or relevant part of the record:

_____

_____

_____

_____

2. Reference Number, if available: _____

3. Any further particulars of the record:

_____

_____

_____

E. Fees

*a) A Request for access to a record, other than a record containing personal information about yourself, will be processed only after a **request fee** has been paid.* *b) You will be notified of the amount of the request fee.* *c) The **fee payable for access** to a record depends on the form in which the access is required, and the reasonable time required to search for and prepare a record.* *d) If you qualify for exemption of the payment of any fee, please state the reason, therefore.*

Reason for exemption of payment of the fee:

_____

_____

F. Form of Access to the Record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in points 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Disability	**Form in which record is required**

Mark the appropriate box with an "X"

Notes:

a) Your indication as to the required form of access depends on the form in which the record is available.

b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.

c) The fee payable for access to the record, if any, will be determined partly by the form in

which access is requested.

1. If the record is in written or printed form:					
	Copy of record		Inspection of record		
2. If the record consists of visual images:					
	View the images		Copy of the images *		Transcription of the image
3. If the record consists of recorded words or information which can be reproduced in sound:					
	Listen to the soundtrack		Transcription of soundtrack		
4. If the record is held on computer or in an electronic or machine-readable form					
	Printed copy of record		Printed copy of information derived from the record *		Copy in computer readable form

If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? **A postal fee is payable**	YES	NO

G. Particulars of right to be exercised or protected:

If the provided space is inadequate, please continue on a separate folio and attach it to this form.

***The requester must sign all the additional folios**.*

Indicate which right is to be exercised or protected:

_____

_____

Explain why the requested record is required for the exercising or protection of the aforementioned right:

_____

_____

H. Notice of decision regarding request for access:

You will be notified in writing whether your request has been approved/denied. If you wish to be informed thereof in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

_____

_____

Signed at_____ this _____ day of _____ 20____

_____

SIGNATURE OF REQUESTER /

PERSON ON WHOSE BEHALF REQUEST IS MADE

APPENDIX 2

REPRODUCTION FEES

Where Access Bank South Africa has voluntarily provided the Minister with a list of categories of records that will automatically be made available to any person requesting access thereto, the only charge that may be levied for obtaining such records, will be a fee for reproduction of the record in question.

Prescribed reproduction fees, as referred to above are:

Description	**Fee**
For every photocopy of an A4-size page or part thereof	R1.10
For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
For a copy in a computer-readable form on: Compact Disk (CD) Flash disk (USB)	 R70.00 R70.00
A transcription of visual images, for an A4-size page or part thereof	R40.00
For a copy of visual images	R60.00
A transcription of an audio record, for an A4-size page or part thereof	R20.00
For a copy of an audio record	R30.00
To search for a record that must be disclosed	R30.00
Where a copy of a record needs to be posted usual postal fee is payable	

Request fees:

Where a requester submits a request for access to information held by a Bank on a person other that the requester himself/herself, a request fee in the amount of R50,00 is payable up-front before Access Bank South Africa will further process the request received.

Access fees:

An access fee is payable in all instances where a request for access to information is granted, except

in those instances where payment of an access fee is specially excluded in terms of PAIA or an exclusion is determined by the Minister in terms of Section 54 (8).

The applicable access fees which will be payable are:

Description	**Fee**
For every photocopy of an A4-size page or part thereof	R 1.10
For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine-readable form	R 0.75
For a copy in a computer readable form on compact disk	R70.00
A transcription of visual images, for an A4-size page or part thereof	R40.00
For copy of visual images	R60.00
A transcription of an audio record, for an A4-size page or part thereof	R20.00
For a copy of an audio record	R30.00
To search for a record that must be disclosed	R30.00
Where a copy of a record needs to be posted usual postal fee is payable	

Deposits:

Where Access Bank South Africa receives a request for access to information held on a person, other than the requester himself/herself and the Information Officer upon receipt of the request is of the opinion that the preparation of the required record of disclosure will take more than 6(six) hours, a deposit is payable by the requester.

The amount of the deposit is equal to 1/3 (one third) of the amount of the applicable access fee.

Note: In terms of Regulation 8, Value Added Tax (VAT) must be added to all fees prescribed in terms of the Regulations.

APPENDIX 3

***FORM 1*: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)**

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	

	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/designated person

APPENDIX 3

***FORM 2*: REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)**

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	

Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a)** **WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b)**

	WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/ designated person

Annexure I EXTERNAL PRIVACY STATEMENT

1. **Introduction**

1.1. For purposes of this Statement:

1. "**Applicable Laws**" means all laws, regulations that Access Bank is required to comply with;

2. "**Client**", "**Supplier**" or "**you**" means any prospective, new or existing client, vendor or Supplier of Access Bank; and

3. "**Access Bank**" or "**we**" or "**us**" means Access Bank Limited and its direct and indirect subsidiaries. To obtain more information in respect of these subsidiaries.

1.2. This Statement sets out how your personal information will be used by Access Bank and applies to any information, including personal and special personal information, you give to Access Bank or which Access Bank may collect from third parties.

1.3. It is important that you read this Statement carefully before submitting any personal information to Access Bank.

1.4. By submitting any personal information to Access Bank you provide consent to the processing of your personal information as set out in this Statement.

1.5. The provisions of this Statement are subject to mandatory, unalterable provisions of Applicable Laws;

1.6. Please do not submit any personal information to Access Bank if you do not agree to any of the provisions of this Statement. If you do not consent to the provisions of this Statement, or parts of the Statement, Access Bank may not be able to provide its products and services to you.

2. **How to contact us**

If you have any comments or questions about this Statement please contact the Information Officer **011 634-4300,** popiInformationofficersa@accessbankplc.com

3. **Amendment of this Statement**

3.1. We may amend this Statement from time to time for any of the following reasons:

1. to provide for the introduction of new systems, methods of operation, services, products, property offerings or facilities;

2. to comply with changes to any legal or regulatory requirement;

3. to ensure that our Statement is clearer and more favourable to you;

4. to rectify any mistake that may be discovered from time to time; and/or

5. For any other reason which Access Bank, in its sole discretion, may deem reasonable or necessary.

3.2. Any such amendment will come into effect and become part of any agreement you have with Access Bank when notice is given to you of the change by publication on our website. It is your responsibility to check the website often.

4. Privacy and indemnity

4.1. Access Bank takes your privacy and the protection of your personal information very seriously, and we will only use your personal information in accordance with this Statement and applicable data protection legislation. It is important that you take all necessary and appropriate steps to protect your personal information yourself (for example, by ensuring that all passwords and access codes are kept secure).

4.2. We have implemented reasonable technical and operational measures to keep your personal information secure.

4.3. **You hereby indemnify and hold Access Bank harmless from any loss, damages or injury that you may incur as a result of any unintentional disclosures of your personal information to unauthorised persons or the provision of incorrect or incomplete personal information to Access Bank.**

5. Information of children

5.1. We do not intend to collect and/or process any personal information of minors, unless we make this clear. If you do provide any personal information to us of children then you warrant that this is done with the consent of the child's parent or guardian to use this information as set out in this Statement.

6. **Suppliers and vendors**

6.1. In the course of our business agreement we may collect personal information about you as a data subject to ensure that the business agreement and matters relating to the agreement can be fulfilled.

6.2. We may also do a due diligence on you to ensure that you meet the requirements set out in our procurement policy.

6.3. If you provide any personal information of other persons to us, such as employees or your directors, you warrant that you are authorised to share their personal information with us for purposes set out in the Statement.

7. **Information which we may collect about you**

7.1. We may collect the following information about you:

1. this information may include your name, address, contact details, date of birth, place of birth, identity number, passport number, bank details, details about your employment, tax number and financial information;

2. records of correspondence or enquiries from you or anyone acting on your behalf;

3. details of transactions you carry out with us;

4. details of contracts, sales or leases you carry out with us;

5. sensitive or special categories of personal information, including biometric information, such as images, fingerprints and voiceprints.

7.2. Where you provide us with the personal information of third parties you should take steps to inform the third party that you need to disclose their details to us, identifying us. We will process their personal information in accordance with this Statement.

8. How we collect information You may provide personal information to us either directly or indirectly (through an agent acting on your behalf, or an introducer), by completing an application form for our products and services or requesting further information about our products and services, whether in writing, through our website, over the telephone or any other means**.**

8.1. We may also collect your personal information from your appointed agent, any regulator, or other third party that may hold such information.

9. **Use of information collected**

9.1. We may use, transfer and disclose your personal information for the purposes of:

1. providing you with the services, products or offerings you have requested, and notifying you about important changes to these services, products or offerings;

2. managing your account or relationship and complying with your instructions or requests;

3. detecting and preventing fraud and money laundering and/or in the interest of security and crime prevention;

4. assessing and dealing with complaints and requests;

5. operational, marketing, auditing, legal and record keeping requirements;

6. verifying your identity or the identify of your beneficial owner;

7. transferring or processing your personal information outside of the Republic of South Africa to countries that may not offer the same level of data protection as the Republic of South Africa, including internationally, for cloud storage purposes, regulatory reporting, reporting to our shareholders and the use of any of our websites and other legitimate interests;

8. complying with Applicable Laws, including lawful requests for information received from local or foreign law enforcement, government and tax collection agencies;

9. recording and/or monitoring your telephone calls and electronic communications to/with Access Bank in order to accurately carry out

your instructions and requests, to use as evidence and in the interests of crime prevention;

10. conducting market research and providing you with information about Access Bank' products or services from time to time via email, telephone or other means (for example, events);

11. where you have unsubscribed from certain direct marketing communications, ensuring that we do not sent such direct marketing to you again;

12. disclosing your personal information to third parties for reasons set out in this Statement or where it is not unlawful to do so;

13. monitoring, keeping record of and having access to all forms of correspondence or communications received by or sent from Access Bank or any of its employees, agents or contractors, including monitoring, recording and using as evidence all telephone communications between you and Access Bank;

14. improving or evaluating the effectiveness of Access Bank' business or products, services or offerings; and

15. prevention and control of any disease.

9.2. We may from time to time (and at any time) contact you about services, products and offerings available from Access Bank or specific subsidiaries which we believe may be of interest to you, by email, phone, text or other electronic means, unless you have unsubscribed from receiving such communications.

10. Disclosure of your information

10.1. Your personal information may be shared with Access Bank' subsidiaries, our agents and sub-contractors, and selected third parties who process the information on our behalf.

10.2. We may also disclose your personal information to third parties in the following circumstances:

1. to any other of Access Bank' subsidiaries, business partners or other third parties to –

- assess and monitor any of your applications for Access Bank' products or services;
- determine which products and services may be of interest to you and/or to send you information about such products and services, unless you object or choose not to receive such communications;
- have a better understanding of your circumstances and needs to provide and improve Access Bank's products and services;
- to any relevant person and/or entity for purposes of prevention, detection and reporting of fraud and criminal activities, the identification of the proceeds of unlawful activities and the combatting of crime;

2. to any regulator or supervisory authority, including those in foreign jurisdictions, if Access Bank in required to do so in terms of Applicable Laws;

- to a prospective buyer or seller of any of our businesses or assets;
- to any person if we are under a duty to disclose or share your personal information in order to comply with any Applicable Laws, or to protect the rights, property or safety of Access Bank, other clients or other third parties; and/or
- to your agent or any other person acting on your behalf, an or an introducer.

10.3. We may transfer your information to another of Access Bank' entities, an agent, sub-contractor or third party who carries on business in another country, including one which may not have data privacy laws similar to those of the Republic. If this happens, we will ensure that anyone to whom we pass your information agrees to treat your information with the same level of protection as if we were dealing with it.

10.4. If you do not wish us to disclose this information to third parties, please contact us at the contact details set out above. We may, however, not be able to provide products or services to you if such disclosure is necessary.

11. **Retention of your information**

We may retain your personal information indefinitely, unless you object, in which case we will only retain it if we are permitted or required to do so in terms of Applicable Laws. However, as a general rule, we will retain your information in accordance with retention periods set out in Applicable Laws, unless we need to retain it for longer for a lawful purpose. (For example, for the purposes of complaints handling, legal processes and proceedings.)

12. **Access to, correction and deletion of your personal information**

You may request details of personal information which we hold about you under the Promotion of Access to Information Act, 2000 ("**PAIA**"). Fees to obtain a copy or a description of personal information held about you are prescribed in terms of PAIA. Confirmation of whether or not we hold personal information about you may be requested free of charge. If you would like to obtain a copy of your personal information held by Access Bank, please review our PAIA Manual located at PAIAsa@accessbankplc.com

12.1. You may request the correction of personal information Access Bank holds about you. Please ensure that the information we hold about you is complete, accurate and up to date. If you fail to keep your information updated, or if your information is incorrect, Access Bank may limit the products and services offered to you or elect not to open the account.

12.2. You have a right in certain circumstances to request the destruction or deletion of and, where applicable, to obtain restriction on the processing of personal information held about you. If you wish to exercise this right, please contact us using the contact details set out above.

12.3. You have a right to object on reasonable grounds to the processing of your personal information where the processing is carried out in order to protect our legitimate interests or your legitimate interests, unless the law provides for such processing.

13. **Complaints**

13.1. Should you believe that Access Bank has utilised your personal information contrary to Applicable Laws, you undertake to first attempt to resolve any concerns with Access Bank.

13.2. If you are not satisfied with such process, you may have the right to lodge a complaint with the Information Regulator, using the contact details listed below:

1. Tel: 012 406 4818

2. Fax: 086 500 3351

3. Email: inforeg@justice.gov.za.

Annexure J WEBSITE PRIVACY POLICY

This website privacy policy describes how we process information we collect and/or receive from you.

1. INFORMATION WE COLLECT AND RECEIVE

We collect and receive information about you in the following ways:

1.1. Information you give us

This includes any information that you provide to us directly:

1.1.1. when you sign-up to utilise our services;

1.1.2. by filling in forms on our websites, or those provided to you;

1.1.3. when you enter a competition, promotion or complete a survey;

1.1.4. by posting comments or content on our social media pages; or

1.1.5. when you contact us, or we contact you and you provide information directly to us.

1.2. What personal information we collect

1.2.1. When you register to use our services, you will be required to provide us with the following information, your

1.2.1.1. name and surname;

1.2.1.2. contact number and email address;

1.2.1.3. physical address;

1.2.1.4. identity or passport number; and

1.2.1.5. date of birth.

1.3. Information we collect or receive when you use our website or social media platforms

We collect information when you use websites or social media platforms by using cookies, web beacons and other technologies. Depending on how you access and use websites, we may receive:

1.3.1. Log information;

1.3.2. Information we infer about you based on your interaction with products and services;

1.3.3. Device information (for example the type of device you're using, how you access platforms, your browser or operating system and your Internet Protocol ("IP") address);

1.3.4. Location information.

1.4. **Information from third-party sources**

We may receive additional information about you that is publicly or commercially available and combine that with the information we have collected or received about you in in other ways.

2. **HOW WE USE THE INFORMATION WE COLLECT AND RECEIVE**

We use the information we collect and receive for the following general purposes:

2.1. to provide you with information, products or services you request from us;

2.2. in order to refer you to an appropriate third-party service provider;

2.3. to communicate with you;

2.4. to provide you with support; and

2.5. to provide effective advertising (for example to be provide you with news, special offers and general information about other goods, services and events which we offer, that are like those that you have already hired or enquired about).

3. **HOW WE SHARE THE INFORMATION WE COLLECT AND RECEIVE**

3.1. We don't sell your personal information to third parties for their marketing purposes.

3.2. We may share information with:

3.2.1. our affiliates, in other words, other companies in our group;

3.2.2. we may disclose your personal information to a limited number of our employees and third party service providers (other than those who we refer you to), who we assist you to interact with;

3.2.3. our business partners. We may share non-personally identifiable information with select business partners;

3.2.4. other parties in response to legal process or when necessary to conduct or protect our legal rights;

3.2.5. companies that provide services to us. Companies that provide services to us or act on our behalf may have access to information about you. These companies are limited in their ability to use information they receive while providing services to us or you; and

3.2.6. third parties where you provide consent. In some cases, third parties (often advertisers) may wish to attain information about you in order to promote their products to you, or for whatever other reason. We may share information with third parties where you provide consent in the form of an explicit opt-in. Before we ask you to opt-in, we will endeavour to provide you with a clear description of what data would be shared with the third-party. Remember that once you have opted in to allow us to send your information to the third-party, we cannot control what they do with your data; therefore, be sure to investigate their privacy policies before providing permission for us to share your information.

4. YOUR RIGHTS

4.1. You have the right to ask us not to contact you for marketing purposes. You can exercise this right at any time by using any of the various "opt-out" options that we will always provide to you when we communicate with you. We won't send you marketing messages if you tell us not to, but we will still need to send you service-related messages.

4.2. Our websites use cookies. If you wish to reject our cookies, you can configure your browser to do so.

4.3. We want to make sure that any data we hold about you is up to date. So, if you think your personal information is inaccurate, you can ask us to correct or remove it.

5. RETENTION OF DATA

We will retain your personal information only for as long as is necessary for the purposes set out in this privacy policy or to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies.

6. OUR COMMITMENT TO SECURITY

The security of your data is important to us. While we strive to use commercially acceptable means to protect your personal information, we cannot guarantee its absolute security. However, we do employ a number of safeguards intended to mitigate the risk of unauthorized access or disclosure of your information. We will do our best to protect your personal information and we will use up to date technology that will help us to do this. We will at all times comply with our obligation under applicable law.

7. TRANSFER OF DATA

7.1. We are based in and operate from South Africa. Your information, including personal information, may be transferred to and maintained on servers located outside of your country of residence, where the data privacy laws, regulations and standards, may not be equivalent to the laws in your country of residence.

7.2. We might transfer your personal information to places outside of South Africa and store it there, where our suppliers might process it. If that happens, your personal information will only be transferred to and stored in country that has equivalent, or better, data protection legislation than South Africa or with a service provider which is subject to an agreement requiring it to comply with data protection requirements equivalent or better than those applicable in South Africa.

7.3. Your use of our website, followed by your submission of information to us, represents your consent to such transfer.

7.4. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

8. LINKS TO OTHER WEBSITES

Our website or social media platforms may contain links to and from websites, mobile applications or services of third parties, advertisers or affiliates. Please note that we are not responsible for the privacy practices of such other parties and advise you to read the privacy statements of each website you visit which collects personal information.

9. CHANGES TO THIS PRIVACY POLICY

We may update this privacy policy from time to time. Any changes that we may make to our privacy policy will be posted on our website and will be effective from the date of posting.

10. ACCESS TO YOUR PERSONAL INFORMATION

10.1. You may at any time request:

10.1.1. confirmation that we hold your personal information;

10.1.2. access to your personal information;

10.1.3. the identities or categories of third parties to whom we have disclosed your personal information; or

10.1.4. that we correct or delete any personal information that is incomplete, misleading, inaccurate, excessive or out of date.

Requests may be made in writing to:

E-mail address: popiInformationofficersa@accessbankplc.com

Annexure K COOKIE POLICY

What are cookies and why do we use them?

We might use cookies and other techniques such as web beacons when you visit our website. "Cookies" are small text files used by us to recognise repeat users, facilitate your on-going access to and use of our website and allow us to track your usage behavior and compile aggregate data that will allow us to improve the functionality of our website and content. "Web beacons" are small, clear picture files used to follow your movements on our website. For example, storing your preferred settings for the next time you visit.

The information we collect from cookies enables us to:

- tailor our websites to your personal needs;
- remember the notifications that you have been shown, so that you are not shown them again;
- help us find information once you have logged in;
- help us link your browsing information to you and your personal information, for example, when you choose to register for a service;
- make improvements and updates to our websites based on the way you want to use them; and
- we generally do not use cookies to identify you personally.

The type of information collected by cookies is not used to personally identify you.

What kind of cookies do we use?

Duration

- Session cookies – These cookies are temporary and expire once you close your browser (or once your session ends).
- Persistent cookies — This category encompasses all cookies that remain on your hard drive until you erase them or your browser does, depending on the cookie's expiration date. All persistent cookies have an expiration date written into their code, but their duration can vary. According to the ePrivacy Directive, they should not last longer than 12 months, but in practice, they could remain on your device much longer if you do not take action.

Provenance

- First-party cookies — As the name implies, first-party cookies are put on your device directly by the website you are visiting.
- Third-party cookies — These are the cookies that are placed on your device, not by the website you are visiting, but by a third party like an advertiser or an analytic system.

Purpose

- Strictly necessary cookies — These cookies are essential for you to browse the website and use its features, such as accessing secure areas of the site. Cookies that allow web shops to hold your items in your cart while you are shopping online are an example of strictly necessary cookies. These cookies will generally be first-party session cookies. While it is not required to obtain consent for these cookies, what they do and why they are necessary should be explained to the user.
- Preferences cookies — Also known as "functionality cookies," these cookies allow a website to remember choices you have made in the past, like what language you prefer, what region you would like weather reports for, or what your user name and password are so you can automatically log in.
- Statistics cookies — Also known as "performance cookies," these cookies collect information about how you use a website, like which pages you visited and which links you clicked on. None of this information can be used to identify you. It is all aggregated and, therefore, anonymized. Their sole purpose is to improve website functions. This includes cookies from third-party analytics services as long as the cookies are for the exclusive use of the owner of the website visited.

  Marketing cookies — These cookies track your online activity to help advertisers deliver more relevant advertising or to limit how many times you see an ad. These cookies can share that information with other organizations or advertisers. These are persistent cookies and almost always of third-party provenance.

  How can you manage your cookie settings?

  To ensure you get the best possible experience when visiting our websites, we recommend that you accept cookies. However, you can opt-out of each cookie category (except strictly necessary cookies) by clicking on the "cookie settings" button or disable cookies in your web browser.

  Cookies may, however, be necessary to provide you with certain features available on our website. If you disable cookies you may not be able to use these features, and your access to our website will be limited.

Annexure L INTERNAL PRIVACY POLICY

1. **What is the purpose of this document?**

1.1. Access Bank South Africa is committed to protecting the privacy and security of your personal information.

1.2. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the requirements of section 18 of the Protection of Personal Information Act, 2013 ("**POPIA**").

1.3. It applies to all employees, workers and contractors.

1.4. Access Bank South Africa is a "responsible party". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

1.5. This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

1.6. It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under POPIA.

2. **Data protection conditions**

2.1. We will comply with POPIA. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.

- Kept only if necessary for the purposes we have told you about.
- Kept securely.

3. **The kind of information we hold about you**

3.1. Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

3.2. There are certain types of more sensitive or special personal data which require a higher level of protection, such as information about a person's health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

3.3. We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.

- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.

3.4. We may also collect, store and use the following more special types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records, including -
    - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Genetic information and biometric data, including fingerprints, photographs and results of psychometric or attainment tests.
- Information about criminal convictions and offences.

4. How is your personal information collected?

4.1. We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties, including former employers, credit reference agencies or bureaus or other background check agencies.

4.2. We may also collect personal information from the trustees or managers of pension arrangements.

4.3. We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

5. **How we will use information about you?**

5.1. We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the employment contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.
- We may also use your personal information in the following situations, which are likely to be rare:
- Where we need to protect your legitimate interests (or someone else's interests).
- Where it is needed for the proper performance of a public law duty.

5.2. <u>Situations in which we will use your personal information</u>

5.2.1. We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in South Africa.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and Unemployment Insurance Fund contributions.
- Providing employee benefits to you.
- Enrolling you in a pension arrangement.
- Liaising with the trustees or managers of a pension arrangement and any other provider of employee benefits.
- Administering the contract, we have entered into with you.
- Business management and planning, including accounting and auditing.

- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Employment equity monitoring.

5.2.2. Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

5.3. <u>If you fail to provide personal information</u>

5.3.1. If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

5.4. Change of purpose

5.4.1. We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

5.4.2. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. How we use particularly sensitive personal information?

6.1. "Special categories" of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed for the establishment, exercise, or defence of a right or obligation under law.

6.2. Less commonly, we may process this type of information where you have already made the information public.

6.3. <u>Situations in which we will use your special personal information</u>

6.3.1. In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. The situations in which we will process your particularly sensitive personal information are listed below. We have indicated the purpose or purposes for which we are processing or will process your more sensitive personal information.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace

adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and statutory insurance. We need to process this information to exercise rights and perform obligations in connection with your employment.

- If you leave our employment and the reason for leaving is determined to be ill-health, injury or disability, we will use information about your physical or mental health, or disability status in reaching a decision about your entitlements to compensation.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful employment equity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

6.4. Do we need your consent?

6.4.1. We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

6.5. Information about criminal convictions

6.5.1. We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our internal privacy policy or data protection policy.

6.5.2. We envisage that we will hold information about criminal convictions.

6.5.3. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

7. Automated decision-making

7.1. Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.
- If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

7.2. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

7.3. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

8. Data sharing

8.1. We may have to share your data with third parties, including third-party service providers and other entities in the group.

8.2. We require third parties to respect the security of your data and to treat it in accordance with the law.

8.3. We may transfer your personal information outside South Africa.

8.4. If we do, you can expect a similar degree of protection in respect of your personal information.

8.5. Why might you share my personal information with third parties?

8.5.1. We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

8.6. Which third-party service providers process my personal information?

8.6.1. "Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration.

8.6.2. We will share personal data relating to your participation in any share plans operated by a group company with third party administrators, nominees, registrars and trustees for the purposes of administering the share plans.

8.6.3. We will share personal data regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

8.7. How secure is my information with third-party service providers and other entities in our group?

8.7.1. We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data We will share personal data relating to your participation in any share plans and pension arrangements operated by a group company with other entities in the group for the purposes of administering the share plans.

8.8. When might you share my personal information with other entities in the group?

8.8.1. We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in

the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data We will share personal data relating to your participation in any share plans and pension arrangements operated by a group company with other entities in the group for the purposes of administering the share plans.

8.9. What about other third parties?

8.9.1. We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

8.9.2. We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to Regulators and shareholders such as directors' remuneration reporting requirements.

8.10. Transferring information outside South Africa

8.10.1. We will possibly transfer the personal information we collect about you to the following country OR countries outside South Africa in order to perform our contract with you: Nigeria

9. **Data security**

9.1. We have put in place measures to protect the security of your information. Details of these measures are available in our PAIA manual.

9.2. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

9.3. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions

and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Information Officer.

9.4. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

10. **Data retention**

10.1. How long will you use my information for?

10.2. We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the Information Officer. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

10.3. In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy OR applicable laws and regulations.

11. **Rights of access, correction, erasure, and restriction**

11.1. Your duty to inform us of changes

11.2. It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

11.3. Your rights in connection with personal information

11.4. Under certain circumstances, by law you have the right to:

- Request access to your personal information as set out in our PAIA manual (commonly known as a "data subject access request"). This

enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

11.5. If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Information Officer in writing.

11.6. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

11.7. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

12. Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Information Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

13. **Information Officer**

We have appointed an Information Officer to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Information Officer. You have the right to make a complaint at any time to the Information Regulator.

14. **Changes to this privacy policy**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy policy, please contact E-mail address: popiInformationofficersa@accessbankplc.com

I,_____ (employee/worker/contractor name), acknowledge that on _____ (date), I received a copy of the Access Bank South Africa's privacy policy for employees, workers and contractors and that I have read and understood it.

Signature …….

Printed Name …….

Annexure M PASSWORD POLICY

Access Bank South Africa Limited

Password policy

1. **DEFINITIONS**

"IO" means the Information Officer of Access Bank South Africa;

"**POPIA**" means the Protection of Personal Information Act 4 of 2013; and

"**Access Bank South Africa staff**" includes all permanent and temporary staff, contractors, and agency workers who have access to Access Bank South Africa systems and are subject to the conditions and scope of this policy.

APPLICATION OF THIS POLICY

This policy applies to all Access Bank South Africa staff, specifically all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Access Bank South Africa facility or has access to the Access Bank South Africa network.

PURPOSE OF THIS POLICY

This document outlines a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords among Access Bank South Africa staff members. Passwords are an important aspect of Access Bank South Africa's computer security as they form the front line of protection for user accounts. A poorly chosen password may result in a compromise of Access Bank South Africa's entire network. As such, all Access Bank South Africa staff are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

GENERAL GUIDELINES

All Active Directory (AD) passwords must be changed at least every 90 days and cannot be reused the past 24 passwords.

Any form of passwords must not be included in email messages or other forms of electronic communication.

PASSWORD HANDLING

Every reasonable effort must be made by all Access Bank South Africa staff to minimise risk of breach /distribution of password(s). This includes adhering to the following password construction requirements:

- Passwords should be a minimum length of 14 characters;
- Passwords should not be a dictionary word or proper name;
- Passwords should not be the same as the User ID;
- Passwords should not be transmitted in the clear or plain text outside secure Access Bank South Africa location(s);
- Passwords should not be displayed when entered; and

UNLAWFUL / PROHIBITED USE

Access Bank South Africa staff are prohibited from the following:

- Revealing password(s) over the phone to anyone;
- Using their user ID as a password;
- Revealing a password in an e-mail or message;
- Revealing a password to a boss/senior;
- Talking about a password in front of others;
- Hinting at the format of a password (e.g., “my family name”);
- Revealing a password on questionnaires or security forms;
- Sharing a password with family members;
- Revealing a password to a co-worker;
- Using the "Remember Password" feature of applications and websites;
- Writing passwords down and storing them anywhere;
- Storing passwords in a file on any unencrypted computer system; and
- Not treating passwords as sensitive and confidential Access Bank South Africa information.

APP DEVELOPERS/ IT

Access Bank South Africa's application developers and/or IT department must ensure that their programs contain the following security precautions:

- Only support the authentication of individual users.
- Not store passwords in clear text or in any easily reversible form.

- Provide some sort of role management, such that one user can take over the function of another without having to know the other's password.

REMOTE ACCESS

Access to the Access Bank South Africa network(s) via remote access is to be controlled by using either a Virtual Private Network (in which a password and user identity are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Access Bank South Africa and Access Bank South Africa staff. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

POLICY REVISION

Monitoring

It is the responsibility of IO and/or anyone mandated by him/her to support and monitor this Policy. Any concerns should be brought to the attention of the IO.

This policy has been reviewed and approved by the IO and is subject to change without prior notice. Password cracking or guessing may be performed on a periodic or random basis, should a password be successfully guessed or cracked during one of these scans, you will be required to change it.

CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Access Bank South Africa LIMITED

BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY

About this policy

1.1. We recognise that many of our staff have personal mobile devices (such as tablets, smartphones and handheld computers), which they could use for business purposes, and that there can be benefits for both us and staff, including increased flexibility in our working practices, in permitting such use. However, the use of personal mobile devices for business purposes gives rise to increased risk in terms of the security of our IT resources and communications systems, the protection of confidential and proprietary information and reputation, and compliance with legal obligations.

1.2. Anyone covered by this policy may use a personal mobile device for business purposes, if they sign the declaration at the end of this policy and adhere to its terms.

1.3. No one is required to use their personal mobile device for business purposes. It is a matter entirely for each person's discretion.

1.4. This policy covers all employees, officers, consultants, contractors, casual workers and agency workers.

1.5. Certain obligations under this policy are contractual and will form part of your contract of employment. These are clearly identified. The remaining sections of this policy do not form part of any employee's contract of employment and we may amend it at any time, including the contractual obligations that it places on staff, or remove the policy entirely, at any time.

2. **Personnel responsible for this policy**

2.1. Our Information Officer has overall responsibility for the effective operation of this policy and shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

2.2. Our Information Officer has responsibility for ensuring that any person who may be involved with administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

2.3. All staff are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the Information Officer.

2.4. If you have any questions regarding this policy or have questions about using your device for business purposes which are not addressed in this policy, please contact the Information Officer.

3. **Scope and purpose of the policy**

3.1. This policy applies to staff who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for business purposes. It applies to use of the device both during and outside office hours and whether or not use of the device takes place at your normal place of work.

3.2. This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers.

3.3. When you access our systems, you may be able to access data about us including information which is confidential, proprietary or private (collectively referred to as company data in this policy).

3.4. When you access our systems using a device, we are exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to our systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.

3.5. The purpose of this policy is to protect our systems and company data, and to prevent company data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

3.6. Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal and in the case of a breach of this policy by a contractor, consultant, casual or agency worker, the termination of the engagement. It may also

lead in some cases to possible criminal charges. Disciplinary action may be taken whether the breach is committed during or outside office hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

3.7. Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist staff in connecting to our systems.

4. **Connecting devices to our systems**

4.1. Connectivity of all devices is centrally managed IT Help Desk, who must approve a device before it can be connected to our systems. You may apply for a device to be added to the approved list by submitting it to IT Help Desk who will have full discretion to approve or reject the device.

4.2. We reserve the right to refuse or remove permission for your device to connect with our systems. IT Help Desk will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, us, our staff, our business connections, our systems, or our company data at risk or that may otherwise breach this policy.

5. **Monitoring**

5.1. The contents of our systems and company data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

5.2. We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device, whether or not the device is in your possession.

5.3. It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, you should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential.

5.4. Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, in order to:

5.4.1. prevent misuse of the device and protect company data;

5.4.2. ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);

5.4.3. monitor performance at work; and

5.4.4. ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

5.5. We may also store copies of any content for a period after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

5.6. By signing the declaration at the end of this policy, you confirm your agreement (without further notice or permission) to such monitoring and to our right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

6. **Security requirements**

6.1. You must comply with our BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY.

6.2. In addition, you must:

6.2.1. at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether it is in use and whether it is

being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device;

6.2.1.1. Always protect the device with a pin number or password and keep that pin number or password secure. The pin number or password should be changed when prompted by the system. If the confidentiality of a pin number or password is compromised, you must change it immediately. The use of pin numbers and passwords should not create an expectation of privacy by you in the device;

6.2.1.2. maintain the device's original operating system;

6.2.1.3. not download and install software to the device;

6.2.1.4. not alter the security settings of the device without our consent;

6.2.1.5. prohibit use of the device by anyone not authorised by us, including your family, friends and business associates;

6.2.1.6. not download or transfer any company data OR ANY CATEGORY OF DATA RESTRICTED to the device, for example via e-mail attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device;

6.2.1.7. not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of company data. Any such backups inadvertently created must be deleted immediately;

6.2.1.8. not use a device to capture images, video, or audio, whether native to the device or through third-party applications, within the workplace;

6.2.1.9. where we have permitted you to store company data on the device, ensure that the company data is encrypted using appropriate encryption technologies approved by the IT Department.

6.2.1.10. not use the device as a mobile hot spot.

6.3. We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the company data on it for legitimate business purposes, which include (without limitation) enabling us to:

6.3.1. inspect the device for use of unauthorised applications or software;

6.3.2. inspect any company data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect company data;

6.3.3. investigate or resolve any security incident or unauthorised use of our systems;

6.3.4. conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

6.3.5. ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

6.4. You must co-operate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal. This paragraph 6.3 of the policy is contractual.

6.5. If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any company data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from company data in all circumstances. You should therefore regularly backup any personal data contained on the device.

6.6. By signing the declaration at the end of this policy, you consent to us, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using some or all of the data on or from a device for the legitimate business purposes set out above.

7. **Lost or stolen devices and unauthorised access**

7.1. In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to IT Security Officer immediately.

7.2. Appropriate steps will be taken to ensure that company data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all company data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from company data in all circumstances. You should therefore regularly backup all personal data stored on the device.

8. **Procedure on termination of employment**

On your last day of work, or your last day before commencing a period of garden leave, all company data (including work e-mails), and any software applications provided by us for business purposes, must not be removed from the device by the IT Security Officer. If this cannot be achieved remotely, the device must be submitted to the IT Security Officer for wiping and software removal. You must provide all necessary co-operation and assistance to the IT Security Officer in relation to this process. This paragraph 8 of the policy is contractual.

9. **Personal data**

We shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless necessary. If such access or copying occurs inadvertently, we shall delete any and all such personal data as soon as it comes to our attention. This limitation does not apply to personal data which is also company data (including personal e-mails sent or received using our e-mail system). For this reason, you are encouraged not to use work e-mail for personal purposes.

10. **Appropriate use**

10.1. You should never access or use our systems or company data through a device in a way that breaches any of our other policies. For example, you must not use a device to

10.1.1. breach our obligations with respect to the rules of relevant regulatory bodies;

10.1.2. breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy;

10.1.3. breach our Disciplinary Rules;

10.1.4. defame or criticise us or our affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;

10.1.5. harass or bully other staff in any way OR breach our Anti-harassment and bullying policy;

10.1.6. unlawfully discriminate against other staff or third parties OR breach our Equal opportunities policy;

10.1.7. breach our Data protection policy]

10.1.8. breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to a device).

10.2. If you breach any of the above policies you may be subject to disciplinary action up to and including dismissal.

10.3. You must not talk, text, e-mail or otherwise use a device while operating a company vehicle or while operating a personal vehicle for business purposes. You must comply with any applicable law concerning the use of devices in vehicles. For your own safety and the safety of others, we recommend you should not use your device while operating vehicles of any kind.

11. **Technical support**

We do not provide technical support for devices. If you use a device for business purposes you are responsible for any repairs, maintenance or replacement costs and services.

12. **Costs and reimbursements**

[You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By signing the declaration at the end of this policy you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.

OR

We will reimburse the actual costs associated with your business usage of the device, including a pro rata portion of any necessary repairs or replacement costs]. To be eligible for reimbursement, you must send a copy of your monthly bill substantiating the costs related to your business usage [and/or a copy of the bill or receipt substantiating any necessary repairs or replacement costs] to [POSITION]. For more information on device reimbursement procedures, please [read our Expenses Policy **OR** contact [POSITION]].

OR

We will reimburse a fixed monthly amount for costs associated with your device usage for business purposes [, including repairs or replacement costs]. If eligible, you will receive:

- [Voice services only: R[AMOUNT] each month.]
- [Data services only: R[AMOUNT] each month.]
- [Voice and data services: R[AMOUNT] each month.]
- [Repair or replacement costs: R[AMOUNT] each [month OR year OR [TIME PERIOD]].]]

To be eligible for reimbursement (which may be a taxable benefit), you must send a copy of your monthly statement or bill substantiating your usage of the device for business purposes to [POSITION]. For more information on device reimbursement procedures, please contact [POSITION].

DECLARATION AND AGREEMENT

I [NAME] wish to use my personal mobile device for business purposes and explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all the terms contained in the Bring Your Own Device to Work Policy.
- I understand that the terms of this policy will always apply to me, during or outside office hours and whether I am at my normal place of work.
- I acknowledge and agree that authorised personnel of Access Bank South Africa shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my personal data).
- I understand and agree that Access Bank South Africa in its discretion may amend or remove this policy at any time and that I will be bound by the terms of the policy as amended.

_____

SIGNED

_____

PRINTED NAME

_____

DATE

Annexure O OPERATOR CLAUSES

[The following clauses should be inserted with the necessary changes to detail into the relevant Access Bank South Africa services-level and non-disclosure agreements.

14. **OPERATOR WARRANTY**

14.1. Should either Party constitute an "Operator" as defined in the Protection of Personal Information Act 4 of 2013 ("**POPIA**") and the other Party a "Responsible Party" as defined in POPIA in respect of any "personal information" as defined in POPIA for purposes in terms or relating to this Agreement ("**Personal Data**"), the Party constituting the Operator shall:

1. process such Personal Data with the knowledge or authorisation of the other Party, in accordance with this Agreement or as required by POPIA and as necessary to perform its obligations under this Agreement and for no other purpose;

2. treat such Personal Data as confidential and not disclose it, unless required by law or during the proper performance of its duties;

3. secure the integrity and confidentiality of such Personal Data by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of Personal Data and unlawful access to or processing of Personal Data;

4. take reasonable measures to -

- identify all reasonably foreseeable internal and external risks to Personal Data;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and

5. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards;

6. have due regard to generally accepted information security practices and procedures which may apply to that Party generally or be required in terms of specific industry or professional rules and regulations; and

7. notify the other Party as soon as reasonably possible after obtaining actual knowledge of reasonable grounds to believe that the Personal Data has been accessed or acquired by any unauthorised person.

15. **INDEMNITY**

The Party which constitutes the Operator hereby indemnifies and holds Access Bank South Africa harmless from any liability whatsoever arising from the Operator's failure to comply with the warranties contained in this Agreement.

Annexure P PHOTOGRAPHY POLICY

1. **INTERPRETATION OF THIS POLICY**

1.1. "**Photograph**" and "**video images**" refer to any kind of image capture, still or moving, obtained by any photographic device including still image cameras, video cameras, webcams and photographic enabled mobile telephones, and any other type of image capture device not specified here, whether digital or not, using technology existent at this time or in the future. The processing (including storage) of such images includes film negative, film positive (e.g. transparencies and slides, movies, etc.), photographic paper, digital media, magnetic tape and any other kind of storage method able to be used for the storage of images, still or moving, available now or in the future;

1.2. "IO" means the Information Officer of Access Bank South Africa; and

1.3. "POPIA" means the Protection of Personal Information Act 4 of 2013.

2. **APPLICATION**

This Policy applies to Access Bank South Africa and its employees and representatives.

3. **PURPOSE**

3.1. The purpose of this Policy is to set out general rules governing the capture and distribution of images and photographs of data subjects, and to give employees of Access Bank South Africa as well as Access Bank South Africa's clients, visitors, suppliers and customers guidelines on how Access Bank South Africa handles their photographic images. This Policy applies to activities on Access Bank South Africa premises and (in certain circumstances) off-site events or trips.

3.2. Access Bank South Africa is cognisant of the fact that there may be a potential risk to the welfare of data subjects when individual persons can be identified in photographs and/or video images. In order to minimise such risk, and to comply with the provisions of POPIA, Access Bank South Africa has developed this Policy.

3.3. Photographs and/or video images of the employees of Access Bank South Africa as well asAccess Bank South Africa's clients, visitors, suppliers and customers are deemed special personal information in terms of POPIA. Therefore, the processing of such photographs and/or video images is subject to strict processing conditions and requires the consent (which may be in electronic format) of either the data subject concerned or in the case of minors, their legal guardian. In addition, and in line with the conditions for lawful processing of personal informal set out in Chapter

3 of POPIA, the IO and/or anyone mandated by him/her to process personal information must make sure the information is:

3.3.1. used fairly and lawfully;

3.3.2. used for its limited, specifically stated purposes;

3.3.3. used in a way that is adequate, relevant and not excessive;

3.3.4. accurate;

3.3.5. kept for no longer than is absolutely necessary;

3.3.6. handled according to people's data protection rights;

3.3.7. kept safe and secure; and

3.3.8. not transferred to a third party outside South Africa without consent from the data subject and adequate data protection provisions from the third party.

3.4. This Policy is part of Access Bank South Africa's strategy for safeguarding the rights of data subjects within our care and should be read in conjunction with our CCTV Monitoring Policy.

4. GENERAL PRINCIPLES

4.1. Data Processing and handling

Every reasonable effort must be made by Access Bank South Africa to minimise risk of inappropriate capture and distribution of photographs and video images. This includes:

4.1.1. securing consent for the use of photographs and/or video images of the data subjects;

4.1.2. not using photographs and/or video images of staff who have left the employ of Access Bank South Africa without their consent;

4.1.3. ensuring that data subject names are not used alongside images in publically-available material without consent;

4.1.4. not using photographs and/or video images of any data subject who is subject to a court order;

4.1.5. storing photographs and/or video images securely and ensuring such images are accessible only by those so authorised;

4.1.6. storing photographs and/or video images securely (whether physical or digital) with appropriate access controls; and

4.1.7. ensuring staff of Access Bank South Africa are appropriately informed about this Policy.

4.2. Photography and image capture within Access Bank South Africa

4.2.1. Photographs and/or video images of data subjects may be captured as part of operational, security and other processes. PIC staff must not take or transmit any recording of data subjects acting in any official capacity at, or representing Access Bank South Africa in any manner, on any personal device, without the IO's consent.

4.2.2. Furthermore, Access Bank South Africa's employees should also be aware that taking photographs of colleagues using personal devices should only happen with the permission of the member of staff in question.

4.2.3. Images of Access Bank South Africa's employees, clients, visitors, suppliers and customers must not be displayed on websites, in publications or in a public place, and in particular on social media platforms, such a Facebook and Instagram, without specific consent. The definition of a public place includes areas where visitors to Access Bank South Africa have access.

4.3. Photography and image capture by others

As a general rule no client, visitor, supplier or customer of Access Bank South Africa is permitted to use a camera (including a mobile phone's camera facility) whilst on Access Bank South Africa's premises. In addition, Access Bank South Africa strongly advises against the publication of any photographs and/or video images on the internet (i.e. on social media), and we will request the removal of any such material if deemed illegal, harmful or inappropriate by Access Bank South Africa in any way.

4.4. Monitoring

It is the responsibility of IO and/or anyone mandated by him/her to support and monitor this Policy. Any concerns should be brought to the attention of the IO.

5. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff of Access Bank South Africa comply with all relevant parts of this Policy. Any failure to comply with this Policy could have serious consequences for PIC and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

6. POLICY REVISION

This Policy has been reviewed and approved by the IO and is subject to change without prior notice.

7. CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Telephone number: 011 634-4300

Annexure Q CCTV MONITORING POLICY

1. ABOUT THIS POLICY

The purpose of this policy is to regulate the use of Closed-Circuit Television (CCTV) to monitor and record images for the purposes of safety and security.

2. APPLICATION AND CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

2.1. This policy applies to all staff of Access Bank South Africa, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and Access Bank South Africa reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. GENERAL PRINCIPLES

3.1. Access Bank South Africa is committed to enhancing the quality of life of its employees by integrating the best practices with regard to workplace safety with the state-of-the-art technology. A critical component of a comprehensive security program is the use of CCTV monitoring.

3.2. CCTV monitoring may be used in public areas by Access Bank South Africa to deter crime and to assist in protecting employees and property.

3.3. Information obtained via CCTV monitoring will be used exclusively for security and law enforcement purposes. Information obtained by CCTV monitoring will only be released when so authorised by the IO.

3.4. CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with existing Access Bank South Africa policies and practices and will be limited to uses that do not violate the reasonable expectation of privacy of data subjects.

3.5. Images and related data collected by CCTV are the property of Access Bank South Africa.

4. **RESPONSIBILITIES**

4.1. The IO is responsible for authorizing all CCTV monitoring for safety and security purposes at Access Bank South Africa and overseeing and coordinating the use of CCTV monitoring equipment at Access Bank South Africa.

4.2. Access Bank South Africa will monitor new developments in the law and industry standards in respect of CCTV monitoring.

5. **PROCEDURES**

5.1. Access Bank South Africa will post signage where appropriate. An example of an appropriate sign is:

By entering these premises, you agree that images are being monitored and recorded for the purposes of crime prevention and public safety. This scheme is controlled by Access Bank South Africa. *For more information, call Access Bank South Africa.*

5.2. Individuals whose images are recorded have a right to view the images of themselves and to be provided with a copy of the images against the payment of a reasonable fee.

5.3. The CCTV systems used by Access Bank South Africa will produce clear images which law enforcement bodies (such as the police) can use to investigate crime and that can easily be taken from the system when required.

5.4. CCTV cameras will be installed in positions where they can record clear images.

5.5. CCTV cameras will be positioned to avoid the capturing of images of persons not visiting the premises and residential housing. Any view given of housing will be no greater than what is available with unaided vision.

5.6. Images recorded by CCTV cameras will be securely stored and may only be accessed by authorised persons.

5.7. Images will not be provided to third parties other than law enforcement bodies.

5.8. Regular checks will be carried out to ensure that CCTV cameras are working properly and produce high-quality images.

5.9. CCTV monitoring will not be used in areas which workers would reasonably expect to be private, such as toilet areas and private offices.

5.10. The CCTV monitoring center will be configured so as to prevent the tampering with or duplicating of information.

5.11. Recorded images will be stored for a period not exceeding 14 days and will then be erased, unless retained as part of a criminal investigation or court proceedings or other legitimate use as approved by the IO.

6. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Access Bank South Africa and its employees. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

7. POLICY REVISION

This policy has been reviewed and approved by the IO, and is subject to change without prior notice.

8. CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Telephone number: 011 634-4300

Annexure R SECURITY COMPROMISES POLICY

1. OVERVIEW

1.1. Security compromises require centralised and swift management and this Security Compromises Policy (policy) outlines a framework for responding to such incidents.

1.2. It is essential for all staff to comply with this policy. Security compromises must be notified to the Regulator and to the affected individuals.

2. APPLICATION AND CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

2.1. This policy applies to all staff of Access Bank South Africa, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and Access Bank South Africa reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. KEY CONSIDERATIONS

3.1. Access Bank South Africa must comply with the Protection of Personal Information Act 4 of 2013 ("**POPIA**") to ensure that measures are taken to keep data secure, including specific legal obligations around dealing with a security compromise. Such legal requirements must be observed in addition to the approach set out in this policy.

3.2. This policy includes guidelines on how to deal with security compromises, including:

- Containment and initial assessment;
- Risk evaluation;
- Breach notification;
- Remedial action; and

- Incident response plan.

4. CONTAINMENT AND INITIAL ASSESSMENT

4.1. An important starting point with any security compromise is to consider what steps are required in order to contain it. For example, if the incident involves a form of intrusion (via either internal or external threats) into Access Bank South Africa systems then containment action could include:

- identification of where the intrusion itself is occurring on the systems;
- closing such weak points to contain the incident; and
- prevention of further impact on data through the compromised systems.

4.2. **Team:** Using the risk classification outlined below, where the incident represents a risk that is categorised as a high or medium risk, then a security compromise management team should convene to address the incident.

4.3. **Team authority and scope:** The team should have appropriate representation from the IO and key departments such as, IT, information security, PR, legal, and should also have enough authority within Access Bank South Africa to investigate and address the incident in accordance with this policy.

4.4. **Legal professional privilege:** Care should be taken to ensure that the investigation is carried out utilising to the maximum extent possible the protection of legal professional privilege. For example, engaging Access Bank South Africa legal team and/or appropriate external counsel from the outset may greatly assist in preserving legal professional privilege.

4.5. **Informing Stakeholders:** The investigation team should consider which other internal stakeholders should be informed of the incident and at what stage in the investigation process they should be informed.

4.6. **Confidentiality:** The investigation team should also consider keeping the investigation confidential from those (internally or externally) that do not need to be made aware of the investigation (either wholly or in part). This will allow the investigation to continue unhindered particularly about further scoping of the incident and any activity around it. This may include, for example, notifying an appropriate law enforcement authority.

5. ASSESSING THE RISKS

5.1. The investigation team should assess the risks arising from the security compromise. The key driver behind identifying the risk is to assess and consider any potential adverse consequences, for example to:

- individuals;
- clients, or
- employees.

5.2. These consequences should consider how serious or substantial the harm might be to anyone within these categories. The risk assessment will inevitably require a classification of the incident (see below) in order to drive the level of response required.

6. INCIDENT CLASSIFICATION

6.1. Incidents should be classified according to severity of risk, considering the following:

6.1.1. **Level 1: High risk of**:

- harm to individuals whose confidentiality or data has been breached;
- reputation damage to Access Bank South Africa;
- legal action from individuals or regulators.

6.1.2. **Level 2: Medium risk of**:

- harm to individuals whose confidentiality or data has been breached;
- reputation damage to Access Bank South Africa;
- legal action from individuals or regulators.

6.1.3. **Level 3: Low risk of:**

- harm to individuals whose confidentiality or data has been breached;
- reputation damage to Access Bank South Africa;

- legal action from individuals or regulators.

- Incident classification will depend on Access Bank South Africa policies on the level of sensitivity ascribed to the personal or other types of information. Sensitivity of information will also depend on the personal circumstances of the individuals concerned.

- Access Bank South Africa should define at the outset what information it considers to be of high sensitivity and ensure all staff members are aware of it, taking into account POPIA's provisions on special categories of personal information.

- ***All security compromises or suspected security compromises*** must be treated seriously.

- Do not do anything to the suspected computer/s or other systems equipment, including turning on or off, or shut down the network unless instructed to do so by Access Bank South Africa Information Security team / Information Officer / legal team].

6.2. In practice the investigation may have an insight into the risk level from addressing the security compromise containment and the initial stages of the assessment (see above). However, this stage to evaluate the risk will require the investigation team to focus on determining factors such as the following (non-exhaustive):

- What information:

- was impacted by the security compromise (risk materialised therefore high risk); or

- could have been subject to impact (risk could have materialised therefore medium risk) as a result of the security compromise?

- Who is affected and what is the likelihood of any harm as a result of the incident?

- Where was the information being processed and handled?

- Which Access Bank South Africa department / area / business / subsidiary / office is responsible for such processing and handling?

- What was determined to be the cause of the security compromise?

- What was determined to be the extent or reach of the security compromise?

6.3. **Regulatory reporting**: The investigation will require consideration of the reporting requirements under POPIA and other South African ancillary rules. For that, the IO should be involved from the outset.

6.4. **Protective Measures**: Other factors of the investigation will focus around whether or not the personal information involved in the incident was subject to specific protective measures. For example:

- Was encryption used?
- What levels of encryption were used?
- Was the encryption technology and the standard used enough to safeguard the individuals against any risks as a result of the breach incident?

6.5. As part of the investigation team's role they will need to establish exactly what information has been compromised and whether the incident took place within the control of Access Bank South Africa or whether the risk materialised within the control of its third parties. In the case of third parties, the team will need to assess what obligations and responsibilities may flow under POPIA and also the contract between Access Bank South Africa and the third party.

7. NOTIFICATION OF SECURITY COMPROMISES

7.1. As a result of the investigations carried out during the evaluation of the risk (see above) Access Bank South Africa may decide it is necessary to report the security compromise to third parties, which may include notifying the incident to:

- The Regulator; or
- Individuals whose personal information was accessed or acquired in the compromise (unless their identity cannot be established).
- Other entities or organisations if required by specific legislation - for example, the South African Police Service, the National Intelligence Agency; and
- Other entities or organisations, on an optional basis - for example customers, if deemed appropriate by the public relations department, senior management and the IO.

7.2. The team should consider seeking appropriate expert advice on the notification requirements.

7.3. The notification to the Regulator and the affected individuals must be made as soon as reasonably possible after the discovery of the compromise, taking into account the time it takes to spend on the initial containment, risk assessment and incident classification stages.

7.4. Notification to the affected individuals may only be delayed if the South African Police Service, the National Intelligence Agency or the Regulator determines that notification will harm a criminal investigation.

7.5. As such, the notifications to the South African Police Service, the National Intelligence Agency or the Regulator will have to be submitted before the affected individuals, and it must include a specific question on whether the notification to the affected individuals should be delayed.

7.6. The notification to the affected individuals must be in writing and communicated to the individual in at least one of the following ways:

- mail;
- e-mail;
- placement on the website of Access Bank South Africa;
- publication in the news media; or
- as may be directed by the Regulator.

7.7. The notification must provide enough information to allow the affected individuals to take protective measures against the potential consequences of the compromise. This may include, if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

8. EVALUATION AND RESPONSE

8.1. **Evaluation:** It is clearly essential for Access Bank South Africa to conduct an appropriate investigation. Access Bank South Africa must then analyse the risks arising from a security compromise and the effectiveness of the systems and controls within Access Bank South Africa questioning why the particular weaknesses or failure points lead to the incident arising. For example, if the security

compromise was caused entirely by or even in part attributed to a systemic problem within Access Bank South Africa then simply containing the security compromise and then continuing on a "business as usual" approach would not be acceptable in the eyes of the Regulator.

8.2. **Response and implementation:** The investigatory team should ensure that the lessons learned from the incident should be incorporated into strengthening the existing controls and procedures around data management and security.

9. INCIDENT RESPONSE PLAN - CHECKLIST

9.1. Access Bank South Africa should have, as an integral element of its security compromise response plan, a documented, methodical approach towards addressing the incident which should include factors such as the following:

9.2. **Evaluation of Risk – Assessing what happened:**

- a determination of what information was involved;
- to establish the cause of the incident and the extent of the security compromise;
- determine who is actually affected by the security compromise;
- consider the extent of which those affected by the security compromise will suffer any harm or otherwise assess the consequences as a result of the breach incident.

9.3. **Containment and initial Assessment:**

- contain the security compromise;
- assign responsibilities to investigate the incident;
- assemble and authorise the investigation team;
- notify defined internal stakeholders;
- consider notification to any other third parties as may be required.

9.4. **Notification:**

- allocate responsibilities;

- seek expert assistance and advice;
- notify the Regulator as soon as reasonably possible after discovering the compromise;
- notify all affected individuals, if identifiable, unless told not to by the Regulator;
- notify by methods such as: mail, email, press release or website publication;
- include enough information in the notification to allow the affected individuals to take protective action against the potential consequences of the compromise.

9.5. **Remedial Action**

- ensure that the risk register for Access Bank South Africa is updated with all incidents and suspects incidents (near-misses);
- update policies and procedures to ensure there will be measures to prevent of future breach incidents of this type;
- review any issues raised around service delivery/third party partners;
- test the revised incident and response plan;
- finalise and implement the revise plan and conduct appropriate training.

10. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Access Bank South Africa and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

11. POLICY REVISION

This policy has been reviewed and approved by the IO and is subject to change without prior notice.

12. CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Telephone number: 011 634-4300

Annexure S SUBJECT ACCESS REQUEST POLICY

1. INTRODUCTION

Access Bank South Africa is required to comply with the requirements of POPIA which gives data subjects the right to ask for a description of the personal information that Access Bank South Africa holds about them.

2. APPLICATION AND CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

2.1. This policy applies to all staff of Access Bank South Africa, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and Access Bank South Africa reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. PURPOSE OF THIS DOCUMENT

3.1. This document outlines the process for dealing with Subject Access Requests that are received by Access Bank South Africa and covers:

3.2. How to identify a Subject Access Request;

3.3. Who is entitled to make one ;

3.4. Who within Access Bank South Africa .is responsible for dealing with them;

3.5. The timescale for responding to one;

3.6. How to assess whether a Subject Access Request is valid;

3.7. How to set the scope of, and conduct any search for, information in response to a Subject Access Request;

3.8. What information should be provided in response to the Subject Access Request; and

3.9. What information may be withheld from a response to the Subject Access Request.

3.10. This document provides guidance only and in the event of a Subject Access Request please contact the IO immediately - please see the list at the end of the note for contact details of the IO.

4. RECEIPT OF SUBJECT ACCESS REQUESTS

4.1. A Subject Access Request may be received by Access Bank South Africa in any of a number of different forms, including a telephone call, email or letter requesting access to personal information. Subject Access Requests generally tend to originate from current or past employees, job applicants, clients or third parties acting on their behalf (particularly where criminal or civil proceedings are involved).

4.2. In the first instance, it may not always be clear that a data subject is making a Subject Access Request. Therefore, it is important to be familiar with this policy to be able to identify a Subject Access Request.

4.3. If you receive what you believe to be a Subject Access Request in any form then it is important that you forward a copy of the request to the IO immediately, who will manage the Subject Access Request.

4.4. In the case of a telephone call, it is best practice to inform the data subject that his/her/its request for information must be made in writing and cannot be processed otherwise. You should also notify the IO that the phone call has taken place.

4.5. Once you have passed the request on to the IO and have received an acknowledgement that it has been received, responsibility for processing the Subject Access Request will be managed by the IO and individuals from the relevant department within Access Bank South Africa (as applicable).

5. TIME PERIOD FOR THE RESPONSE

5.1. Access Bank South Africa must respond to a valid Subject Access Request within a reasonable period but always within 30 days.

5.2. Where a Subject Access Request is missing any of its required elements, it is essential that a prompt request for the missing part(s) is sent back to the data subject asking for the missing elements.

5.3. Once all of the requirements set out above have been met and the request has become a valid Subject Access Request, the stated period for providing a formal response must be complied with.

6. WHO IS ENTITLED TO MAKE A SUBJECT ACCESS REQUEST?

6.1. Any data subject is entitled to make a Subject Access Request to Access Bank South Africa. Access Bank South Africa will typically receive Subject Access Requests:

6.2. from its employees or former employees or job applicants;

6.3. from an individual working for a supplier or a supplier;

6.4. from a customer who is an individual or a customer; or

6.5. from an individual that has used Access Bank South Africa website.

6.6. These individuals and entities have a right to be informed by Access Bank South Africa whether personal information about them is being processed. If personal data is being processed in almost any way by Access Bank South Africa then the data subject is entitled to be given any of the following information:

6.7. a description of the personal information held; and

6.8. an indication of all the third parties or categories of third parties who have or have had of access to the information.

Validity of a Subject Access Request

6.9. It is necessary to confirm that the Subject Access Request is valid. The validity of a Subject Access Request will depend on the format and content of the Request. A valid Subject Access Request:

6.10. is in writing to Access Bank South Africa physical or postal address, fax number or e-mail address;

6.11. provides sufficient information to allow the identification of the individual requesting the personal information and the information requested;

6.12. indicates the form in which the information should be provided;

6.13. specifies an address, fax number or email address of the data subject in South Africa; and

6.14. includes sufficient identification of the individual to which the Subject Access Request relates.

7. IDENTIFICATION AND SEARCH TERMS

7.1. The IO must confirm the identity of the individual making the request - i.e. to confirm the person is who the person says it is.

7.2. Where the Subject Access Request is made by an employee or a former employee then this will normally be straightforward. The information to be requested will usually be the employee's/former employee's:

- Employee ID;
- Department;
- Room or Desk number; and / or
- Employee's telephone extension.

7.3. Where the Subject Access Request is made by someone other than an employee or a former employee then you should send a letter requesting confirmation of identity and also requesting, if necessary, further information to be provided to assist in focussing the search for information.

8. SETTING THE SCOPE AND CONDUCTING THE SEARCH

8.1. Subject Access Requests sometimes clearly identify specific information sought by the individual. This permits a simple and targeted search for that information.

8.2. However, other requests are expressed more widely and may, for example, simply request all information held about them (e.g "Please send me a copy of all the information you have on me"). Such a wide-ranging request would be difficult and onerous to comply with given the volume of information that would have to be reviewed.

8.3. When a wide-ranging request is made then the first step is always to contact the individual and try to obtain clarifications about the information that they actually want. This may often result in a much more specific request leading to a much more targeted search.

8.4. Typically, requests may focus on copies of interview notes, employment application forms, personnel files, appraisal information, holiday and leave information, CCTV footage and emails. However, if the individual is not prepared to focus their request then you should use the "Default Access Bank South Africa Search Parameters" set out below.

8.5. In most cases:

8.5.1. the search should include any centrally-held personnel files about the individual (such as Access Bank South Africa employee personnel file);

8.5.2. general and non-specific requests (e.g. for the provision of "all" information held about an individual) are not acceptable. The request must relate to specific personal information;

8.5.3. if the search relates to emails then it should only apply to a limited number of email accounts over a limited period. Keyword searching may also be used; and

8.5.4. it is not necessary to restore back-up information in order to respond to the request unless the individual has a real need for specific information contained in the back-ups.

8.5.5. In general, when setting the parameters for a search, you must consider whether this constitutes a reasonable and proportionate search. This will generally depend on the circumstances but you should consider:

8.5.6. The likelihood that the information exists (i.e. is it just a "fishing expedition"?);

8.5.7. The value or importance of the information to the individual;

8.5.8. The cost of locating and reviewing the information; and

8.5.9. Whether the information is intended for use in litigation (while pending litigation doesn't invalidate a Subject Access Request, it may be more appropriate for disclosure to be made during discovery).

9. THE DEFAULT SEARCH PARAMETERS FOR ACCESS BANK SOUTH AFRICA

9.1. The Default Search Parameters attempt to take into account the above to provide a reasonable and proportionate response so searches for a general request for access to personal information should generally be based on the following parameters

(noting that the specific facts on each request may dictate other search factors), however this may vary from request to request:

9.1.1. A copy of the data subject's personnel file should be provided (in the case of an employee or a former employee);

9.1.2. Pre-defined keywords should be used to search email;

9.1.3. There should be no restoration of back up data without the prior approval of the IO.

9.2. It is important to note that any emails sent internally about the Subject Access Request itself will usually not need to be included in the response, on the basis that they may be legally privileged.

10. IT DEPARTMENT ASSISTANCE FOR ELECTRONIC RECORDS

10.1. The search may require the assistance of other departments, such as the IT department for tracking.

10.2. The IO should define a specific form to be used when requesting assistance from other department, which should set out clearly:

10.2.1. the names of the inbox owners;

10.2.2. the date range (no longer than [6 months] from the date that the valid Subject Access Request was received); and

10.2.3. relevant search terms and parameters.

11. WHICH INFORMATION THAT IS FOUND IN THE SEARCH MUST BE DISCLOSED AND WHAT CAN ACCESS BANK SOUTH AFRICA REFUSE TO DISCLOSE?

11.1. A Subject Access Request only entitles the individual to access personal information about himself/herself. In general, personal information about an individual is required to be disclosed if it identifies that individual.

11.2. However there are important exemptions which may apply. These exemptions apply to very specific information and are complex in its interpretation. The IO will analyse the retrieved personal information and shall apply any relevant exemption.

11.3. Such exemptions may, for example, include information:

11.3.1. That is subject to legal professional privilege; or

11.3.2. That reveals the identity of a third party individual.

12. OTHER INFORMATION TO BE INCLUDED IN THE RESPONSE

The individual is also entitled to information about the third parties or categories of third parties who have or have had access to his / her personal information.

13. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Access Bank South Africa and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

14. POLICY REVISION

This policy has been reviewed and approved by the IO, and is subject to change without prior notice.

15. CONTACT DETAILS OF THE IO

Name: Brendan Van Zyl

Address: Access Bank South Africa, P.O. Box 784921, Sandton, 2146

E-mail address: popiInformationofficersa@accessbankplc.com

Annexure T EMPLOYEE CONTRACT / JOB APPLICATION FORM MODEL CLAUSES

These provisions must be given to all job applicants. Access Bank South Africa should give copies of these provisions to its recruitment agents and all job applicants should be required to return the signed clauses to the Access Bank South Africa along with their CVs. The clauses should also be included in the employment contract and be signed by existing employees.

Consent to Processing of Personal Information

I agree that personal information about me may be processed (including recorded and stored and kept for as long as it required by the employer and processed by the employer for its legitimate interests) subject to the provisions of applicable data protection legislation and the internal privacy policy.

Consent – Credit and Criminal Record

I hereby consent and authorise the employer or its duly authorised agent to make my name, surname, identity number and fingerprints available to the Police Services and/ or any credit bureau and I hereby authorise the employer to conduct any credit references and/or to conduct criminal record enquiry as the employer in its sole discretion deems necessary.

I furthermore authorise the Police Services to furnish personal information regarding my criminal background, criminal history, previous convictions and/or any other relevant information such as usually furnished by the Police Services in this regard, to the employer and/or the employer's duly authorised agent.

I furthermore unconditionally indemnify the Police Services and all its members, employees as well as the Government of against any liability which results or may result from furnishing information in this regard.

I understand that -

a) the information is furnished solely for the purpose of my proposed employment/continuation of my employment with the employer;

b) any information furnished to the employer/the employer's duly authorised agent, will be disclosed to me for comments before a decision is made on my employment/application; and

c) employer/the employer's duly authorised agent is responsible for verifying the accuracy, in every respect, of the information furnished by the Police Services.

Consent – Employment References

I hereby consent and authorise the employer or its duly authorized agent to contact any of my references and to make enquiries in respect of my behaviour, work ethic, competence, expertise, work record, honesty and any related matters as the employer in its sole discretion deems necessary.

Consent – Qualification Verification

I hereby consent and authorise the employer or its duly authorised agent to verify any and all of my qualifications against any source as the employer in its sole discretion deems necessary.

Consent – Psychometric or Other Assessment Testing

I hereby consent and authorise the employer or its duly authorised agent to conduct any employment screening tests on me, including but not limited to, psychometric and other assessment tests, as the employer in its sole discretion deems necessary.

Consent – Special Personal Information

I hereby consent and authorise Access Bank South Africa or its duly authorised agent to process my special personal information, including biometric information, such as photos, images and fingerprints on emails, through CCTV cameras, for purposes of identification and criminal checks and the like, and my health information for purposes of assessing sick leave claims, preventing or controlling disease or illness and the like, as Access Bank South Africa in its sole discretion deems necessary.

Consent – Social Media Scans

I hereby consent and authorise Access Bank South Africa or its duly authorised agent to conduct social media scans, which may involve the processing of my personal information, as Access Bank South Africa in its sole discretion deems necessary.

Consent – Third Party Processing and Further Processing

I hereby consent and authorise the employer or its duly authorised agent to share my personal information, including the information contained in my CV, and/, or information related to the information in this application form, with third parties, where it is in the legitimate interests of the employer or such third parties to do so, including but not limited to, other companies within Access Bank South Africa and recruitment agencies, training facilities and persons who approach Access

Bank South Africa to confirm my employment and/or salary status and/or for reference purposes, and I hereby consent and authorise such third parties to process my personal information for reasons that are related to the legitimate interests of the employer or such third parties.

Consent – Monitoring of Communications

I hereby consent and authorise Access Bank South Africa to monitor my communications, including email, at work.

Consent – Transborder Transfers of Personal Information

I hereby consent and authorise Access Bank South Africa or its duly authorised agent to transfer my personal information to countries outside South Africa for employment-related or storage purposes, including travelling, visa processing, training and cloud storage.

Warranty – Accuracy of Information

I hereby agree to give (where applicable) honest, accurate and current information to Access Bank South Africa and to maintain and update such information when necessary and I hereby indemnify Access Bank South Africa for any harm, loss or damages I may incur due to Access Bank South Africa's reliance on incorrect information relating to me.

Signature: _____
who warrants that he / she is duly authorised thereto

Name: _____

Date: _____

Place: _____

Witness: _____

Witness: _____

F. Applicable legislation and policies

In alphabetical order, list the authorizing and related legislative documents (e.g. acts, regulations, standards), and related Access Bank South Africa policies, procedures, templates, guidelines or committee terms of reference that together form a framework to enable readers to better understand the policy and its context.

Notice should be taken of the following legislation:

Access Bank PLC policies

Access Bank South Africa policies

G. Approval and review process

This policy is reviewed annually, or when legislation changes, by the IO to ensure it is achieving its stated objectives

H. Definitions and abbreviations

Definitions

"Data subjects"	for the purpose of this policy include all living individuals and juristic persons about whom Access Bank South Africa holds personal information. All data subjects have legal rights in relation to their personal information.
"Access Bank South Africa"	means Access Bank South Africa Limited and all its subsidiaries and business areas
"IO"	means the information officer appointed as such by Access Bank South Africa in terms of section 56 of POPIA and who will have the ultimate responsibility to ensure that Access Bank South Africa complies with the provisions of POPIA.
"Operators"	include any person who processes personal information on behalf of a responsible party. Employees of responsible parties are excluded from this definition but it could include suppliers which handle personal information on Access Bank South Africa behalf
"Personal information"	means information relating to an identifiable, living, natural person, and (where applicable) an identifiable, existing juristic person, including the

	name, race, gender, marital status, address and identifying number of a person, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
"POPIA"	means the Protection of Personal Information Act 4 of 2013
"Processing"	is any activity that involves use of personal information. It includes any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as restriction, degradation, erasure or destruction of information.
"Processing conditions"	are the 8 (eight) conditions for the lawful processing of personal information set out in chapter 3 of POPIA.
"Regulator"	means the Information Regulator established in terms of section 39 of POPIA.
"Responsible parties"	are the people who or organisations which determine the purposes for which, and the manner in which, any personal information is processed. They have a responsibility to establish practices and policies in line with POPIA. Access Bank South Africa is the responsible party of all personal information used in its business. Each subsidiary of Access Bank South Africa would be a responsible party in its own right.
"Special personal information"	includes personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

"Users"	include employees whose work involves using personal information. Users have a duty to protect the information they handle by following Access Bank South Africa data privacy and data protection policies at all times.

Abbreviations

I. Review Tracker- History of the Policy

Distribution List:

Name	Department

Version History:

Version	Date	Descriptions	Author(s):
1	February 2019	New Policy	Edward Nathan Sonnenberg Attorneys
2	1 May 2021	Revised version	Edward Nathan Sonnenberg Attorneys

Approval:

Version	Date	Name	Department
1	February 19	ACC and BoD	
2	T.B.A	T.B.A	