CIB (Pty) Ltd Policy in terms of the Protection of Personal Information Act, No. 4 2013 (South Africa) (POPI Act)	
Organisation	CIB (Pty) Ltd
Scope of policy	This policy applies to the business of CIB (Pty) Ltd wherever it is conducted but based at the registered office. It applies to paid staff.
Policy operational date	1 July 2021
Date approved by Information Officer	12 July 2023
Next policy review date	1 July 2024
Introduction	
Purpose of policy	The purpose of this policy is to enable CIB (Pty) Ltd to: • comply with the law in respect of the data it holds about individuals; • follow good practice; • protect CIB (Pty) Ltd 's staff and other individuals • protect the organisation from the consequences of a breach of its responsibilities.
Personal information	This policy applies to information relating to identifiable individuals, in terms of the Protection of Personal Information Act, 2013 (hereinafter POPI Act).
Definitions	All terms used in this policy are as stipulated in the POPI Act.
Policy statement	CIB (Pty) Ltd will: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently CIB (Pty) Ltd recognises that its first priority under the POPI Act is to avoid causing harm to individuals. In the main this means: • keeping information securely in the right hands, and

	• holding good quality information. Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, CIB (Pty) Ltd will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.
Key risks	CIB (Pty) Ltd has identified the following potential key risks, which this policy is designed to address: • Breach of confidentiality (information being given out inappropriately) • Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed • Failure to offer choice about data use when appropriate • Breach of security by allowing unauthorised access • Harm to individuals if personal data is not up to date • Data Operator contracts
Information Officer Responsibilities	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 1, and Chapter 5, Part B.
Information Officer Responsibilities	The Information Officer has the following responsibilities: • Developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of the POPI Act, including but not limited to the following: • Reviewing the POPI Act and periodic updates as published • Ensuring that POPI Act induction training takes place for all staff • Ensuring that periodic communication awareness on POPI Act responsibilities takes place • Ensuring that Privacy Notices for internal and external purposes are developed and published • Handling data subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Operators • Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of personal information

	• Ensuring that appropriate Security Safeguards in line with the POPI Act for personal information are in place • Handling all aspects of relationship with the Regulator as foreseen in the POPI Act Provide direction to any Deputy Information Officer if and when appointed
Appointment	The appointment of the CIB (Pty) Ltd Information Officer and Deputy Information Officers will be authorised by the Designated Head. Consideration will be given an annual basis of the re-appointment or replacement of the Information Officer; the need for any Deputy to assist the Information Officer.
Processing Limitation	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 2.
Processing Limitation	CIB (Pty) Ltd undertakes to comply with the POPI Act, Conditions 2 in terms of processing limitation, sections 9 to 12, subject to the following stipulation (Forms of Consent).
Forms of consent	CIB (Pty) Ltd undertakes to gain written consent where appropriate; alternatively, a recording must be kept of verbal consent.
Nature of Personal Information	CIB (Pty) Ltd has used the POPI-Personal Information Diagnostic tool to identify all instances of personal information in the organisation.
Purpose specification	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 3.
Purpose specification	CIB (Pty) Ltd undertakes to comply with the POPI Act, Conditions 3 in terms of processing limitation, sections 13 and 14, subject to the following stipulation (Retention periods).
Retention periods	CIB (Pty) Ltd will establish retention periods for at least the following categories of data:

	• Directors • Staff • Customers/policyholders • Suppliers Detailed coverage of the relevant retention periods has been documented in the Personal Information Diagnostic tool.
Further processing limitation	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 4.
Further processing limitation	CIB (Pty) Ltd undertakes to comply with the POPI Act, Conditions 2 in terms of processing limitation, section 15.
Information quality	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 5. CIB (Pty) Ltd will comply with all of the aspects of Condition 5, section 16.
Accuracy	CIB (Pty) Ltd will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular: • ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data. • Data on any individual will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets. • Effective procedures will be in place so that all relevant systems are updated when information about any individual changes. • Staff who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
Updating	CIB (Pty) Ltd will review all personal information on an annual basis in June of each year.
Archiving	Archived electronic records of CIB (Pty) Ltd are stored on existing

	systems. Emails are archived on Mimecast and on the exchange server. Paper record archiving takes place using onsite storage and are destroyed and certified by Document & Data Shredding Technologies (Pty) Ltd.
Openness	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 6.
Openness	In line with Conditions 6 and 8 of the Act, CIB (Pty) Ltd is committed to ensuring that in principle Data Subjects are aware that their data is being processed and • for what purpose it is being processed; • what types of disclosure are likely; and • how to exercise their rights in relation to the data.
Procedure	Data Subjects will generally be informed in the following ways: • Staff: through this policy • Customers, Suppliers and other interested parties: through the CIB (Pty) Ltd Privacy Notice Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.
Security Safeguards	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 7, section 19 to 22. This section of the policy only addresses security issues relating to personal information. It does not cover security of the building, business continuity or any other aspect of security.
Specific risks	CIB (Pty) Ltd has identified the following risks: • Staff with access to personal information could misuse it. • Staff may be tricked into giving away information, either about customers / suppliers or colleagues, especially over the

	phone, through “social engineering”.
Setting security levels	Access to information on the main CIB (Pty) Ltd computer system will be controlled by function. CIB (Pty) Ltd has used the POPI-Personal Information Diagnostic tool to identify security levels required for each record held which contains Personal Information.
Security measures	CIB (Pty) Ltd will ensure that all necessary controls are in place in terms of access to personal information.
Business continuity	CIB (Pty) Ltd will ensure that adequate steps are taken to provide business continuity in the event of an emergency.
Related policy	Please see the CIB (Pty) Ltd Information Security Policy for further guidance.
Data Subject participation	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 8, sections 23 to 25.
Responsibility	Any subject access requests will be handled by the POPI Act Information Officer in terms of Condition 8.
Procedure for making request	Subject access requests must be in writing. All staff are required to pass on anything which might be a subject access request to the POPI Act Information Officer without delay. Requests for access to personal information will be handled in compliance with the POPI Act and in compliance with the Promotion of Access to Information Act (PAIA), as defined in the CIB (Pty) Ltd PAIA Manual.
Provision for verifying identity	Where the individual making a subject access request is not personally known to the POPI Act Information Officer their identity will be verified before handing over any information.
Charging	Fees for access to personal information will be handled in compliance with the PAIA Act.

Procedure for granting access	Procedures for access to personal information will be handled in compliance with the PAIA Act, as defined in the CIB (Pty) Ltd PAIA Manual.
Processing of Special Personal Information	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Part B, sections 26 to 33.
Processing of Special Personal Information	CIB (Pty) Ltd has the policy of adhering to the process of Special Personal Information which relates to 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. Special personal information includes criminal behaviour relating to alleged offences or proceedings dealing with alleged offences. Unless a general authorisation, alternatively a specific authorisation relating to the different types of special personal information applies, a responsible party is prohibited from processing special personal information.
Processing of Personal Information of Children	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Part C, sections 34 and 35.
Processing of Personal Information of Children	CIB (Pty) Ltd has the policy of adhering to the process of Special Personal Information of children only applies for under-18 individuals, so age check is required for all personal information records. General authorisation concerning personal information of children only applies where under-18 involved. CIB (Pty) Ltd has used the POPI-Personal Information Diagnostic tool to identify any records held which contain Personal Information of children.
Prior Authorisation	
Scope	The scope of this aspect of the policy is defined by the provisions of

	the POPI Act, Chapter 6.
Prior Authorisation	CIB (Pty) Ltd has the policy of adhering to the process of Prior Authorisation in terms of sections 57 to 59.
Transborder information flows	
Scope	The scope of this aspect of the policy is defined by the provisions of the POPI Act, Chapter 9.
Transborder information flows	CIB (Pty) Ltd will ensure that the POPI Act Chapter 9, section 72 is fully complied with. CIB (Pty) Ltd has used the POPI-Personal Information Diagnostic tool to identify Transborder flows which contain Personal Information. Compliance with section 72 will be achieved through the use of the necessary contractual commitments from the relevant parties.
Staff training & acceptance of responsibilities	
Scope	The scope of this aspect of the policy is written in support of the provisions of the POPI Act, Chapter 5, Part B.
Documentation	Information for staff is contained in this policy document and other materials made available by the Information Officer.
Induction	The CIB (Pty) Ltd Information Officer will ensure that all staff who have access to any kind of personal information will have their responsibilities outlined during their induction procedures.
Continuing training	CIB (Pty) Ltd will provide opportunities for staff to explore POPI Act issues through training, team meetings, and supervisions.
Procedure for staff signifying acceptance of policy	CIB (Pty) Ltd will ensure that all staff sign acceptance of this policy once they have had a chance to understand the policy and their responsibilities in terms of the policy and the POPI Act.
Policy review	
Responsibility	The CIB (Pty) Ltd Information Officer is responsible for an annual review to be completed prior to the policy anniversary date.

Procedure	The CIB (Pty) Ltd Information Officer will ensure relevant stakeholders are consulted as part of the annual review to be completed prior to the policy anniversary date.
List of Policies relevant to POPIA	
Website Privacy Policy	See Annexure A
CCTV Camera Policy	See Annexure B
Password Policy	See Annexure C
Bring Your Own Device Policy	See Annexure D
Personal Information Sharing Policy	See Annexure E
Printing Policy	See Annexure F
Subject Access Request Policy	See Annexure G
Data Protection Policy	See Annexure H
Security Compromises Policy	See Annexure I
Cookies Policy	See Annexure J
Record Retention Policy	See Annexure K
IT Security Policy	See Annexure L
Privacy Policy	See Annexure M
Clean Desk Policy	See Annexure N

Annexure A

WEBSITE PRIVACY POLICY

INTRODUCTION

We respect the privacy of everyone who visits this website. Accordingly, we would like to inform you about the way we could use any Personal Information that you may provide during your visit. At CIB we are committed to protecting your privacy and to ensure that your Personal Information is collected and used properly, lawfully and openly.

We recommend you read the Customer Privacy Notice and Consent policy ("Customer Privacy Notice and Consent" available at www.cib.co.za) so that you understand our approach towards the use of your Personal Information. By submitting your Personal Information to us, you will be deemed to have given your permission – where necessary and appropriate – for processing referred to in this policy. By using this website, you acknowledge that you have reviewed the terms of the Customer Privacy Notice and Consent to the use of Personal Information and agree that we may collect, use and transfer your Personal Information in accordance therewith.

If you do not agree with these terms, you may choose not to use our website, and not provide any Personal Information through the site.

The Customer Privacy Notice and Consent forms part of our Site Terms and Conditions of use and such shall be governed by and construed in accordance with the laws of South Africa in particular the Protection of Personal Information Act, 2013 (POPI Act).

Definitions

For the purposes of this Privacy Notice, the following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Affiliate means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.

Account means a unique account created for you to access our Service or parts of our Service.

Company (referred to as either "the Company", "we", "us" or "our" in this Notice) refers to CIB (Pty) Ltd, Riley Road 15E, Riley Road Office Park.

Cookies are small files that are placed on your computer, mobile device or any other device by a website, containing the details of your browsing history on that website among its many uses.

Country refers to South Africa

Device means devices that have components for controlling the flow of electrical currents for the purpose of information processing and system control.

Personal Information according to the POPI Act, means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. The POPI Act, which has

more specific examples if you need them, can be found at the following link: www.gov.za/documents/download.php?f=204368

Service refers to the CIB website.

Service Provider means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analysing how the Service is used.

Third-party Social Media Service refers to any website or any social network website through which a user can log in or create an account to use the Service.

Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

Website refers to CIB, accessible from https://www.cib.co.za/

you (also "your") means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.

Personal versus non-Personal Information

Personal Information

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- Address, State, Province, ZIP/Postal code, City (and/or geolocation)
- user-generated content, posts and other content you submit to our web site

With your consent, we may also supplement the information that you provide to us with information we receive from other companies in order to offer you a more consistent and personalised experience in your interactions with CIB.

Non – Personal Information

Usage Data is collected automatically when using the Service. Usage Data may include information such as your Device's Internet Protocol address, browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

We may automatically collect non-Personal Information about you such as the type of internet browsers you use or the website from which you linked to our website. we may also aggregate details which you have submitted to the site (for example, the products or services you are interested in). You cannot be identified from this information and it is only used to assist us in providing an effective service on this web

site. We may from time-to-time supply third parties with this non-personal or aggregated data for uses in connection with this website.

When you access the Service by or through a mobile device, we may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile device's unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

We may also collect information that your browser sends whenever you visit our Service or when you access the Service by or through a mobile device.

Tracking Technologies and Cookies
We use Cookies and similar tracking technologies including beacons, tags, and scripts to track the activity on our Service.

You can instruct your browser to refuse all Cookies or to just indicate when a Cookie is being sent. However, if you do not accept Cookies, you may not be able to use some parts of our Service.

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on your personal computer or mobile device when you go offline, while Session Cookies are deleted as soon as you close your web browser.

We use both Session and Persistent Cookies for the purposes set out below:

Session Cookies
These Cookies are essential to provide you with services available through the website and to enable you to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that you have asked for cannot be provided, and we only use these Cookies to provide you with those services.

Persistent Cookies
Cookies Policy / Notice Acceptance Cookies

These Cookies identify if users have accepted the use of Cookies on the website.

Functionality Cookies

These Cookies allow us to remember choices you make when you use the website, such as remembering your login details or language preference. The purpose of these Cookies is to provide you with a more personal experience and to avoid you having to re-enter your preferences every time you use the website.

Use of your Personal Information
The Company may use Personal Information for the following purposes:

To provide and maintain our Service, including to monitor the usage of our Service.
To manage your registration as a user of the Service. The Personal Information you provide can give you access to different functionalities of the Service that are available to you as a registered user.
For the performance of a contract iro the development, compliance and undertaking of the purchase contract for the products, items or services you have purchased or of any other contract with us through the Service.

To contact you by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
To provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information.
To attend and manage your requests to us.
To confirm and verify your identity or to verify that you are an authorised customer for security purposes
To carry out our obligations arising from any contracts entered into between you and us
To notify you about changes to our service
For market research purposes
To assist with business development
For the detection and prevention of fraud, crime, or other malpractice
To conduct market or customer satisfaction research or for statistical analysis
For audit and record keeping purposes
In connection with legal proceedings
To comply with legal and regulatory requirements or industry codes to which we subscribe or which apply to us, or when it is otherwise allowed by law.
For monitoring and auditing site usage
Evaluate the use of the site, products and services
Analyse the effectiveness of our advertisements, competitions and promotions
Personalise your website experience, as well as to evaluate (anonymously and in the aggregate) statistics on website activity, such as what time you visited it, whether you've visited it before and what site referred you to it
Make the site easier to use and to better tailor the site and our products to your interests and needs
Help speed up your future activities and experience on the site. For example, a site can recognise that you have provided your Personal Information and will not request the same information a second time.
Collect information about the device you are using to view the site, such as your IP address or the type of Internet browser or operating system you are using, and link this to your Personal Information so as to ensure that the site presents the best web experience for you

Sharing of Personal Information

We may disclose your Personal Information to our service providers who are involved in the delivery of products or services to you. We have agreements in place to ensure that they comply with these privacy terms.

We may share your personal information with Service Providers to monitor and analyse the use of our Service, to show advertisements to you to help support and maintain our Service, to contact you, to advertise on third party websites to you after you visited our Service or for payment processing.
We may share or transfer your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of our business to another company.

We may share your information with our affiliates, in which case we will require those affiliates to honour this Privacy Notice. Affiliates include our parent company and any other subsidiaries, joint venture partners or other companies that we control or that are under common control with us.
We may share your information with our business partners to offer you certain products, services or promotions.
When you share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If you interact with other users or register through a Third-Party Social Media Service, your contacts on the Third-Party Social Media Service may see your name, profile, pictures and description of your activity. Similarly, other users will be able to view descriptions of your activity, communicate with you and view your profile.
We may also disclose your information:

- Where we have a duty or a right to disclose in terms of law or industry codes;
- Where we believe it is necessary to protect our rights.

Retention of Personal Information

The Company will retain your Personal Information only for as long as is necessary for the purposes set out in this Privacy Notice. we will retain and use your Personal Information to the extent necessary to comply with our legal obligations (for example, if we are required to retain your Information to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.
The Company will also retain usage Data for internal analysis purposes. usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this data for longer time periods.

Transfer of Personal Information

Your information, including Personal Information, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

Your consent to this Privacy Notice followed by your submission of such information represents your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this Privacy Notice and no transfer of your Personal Information will take place to an organisation or a country unless there are adequate controls in place including the security of your information and other personal information.

Disclosure of Personal Information

If the Company is involved in a merger, acquisition or asset sale, your Personal Information may be transferred. we will provide notice before your Personal Information is transferred and becomes subject to a different Privacy Notice.
Under certain circumstances, the Company may be required to disclose your Personal Information if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).
The Company may disclose your Personal Information in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of users of the Service or the public
- Protect against legal liability

Correction of Personal Information

You have the right to ask us to update, correct or delete your personal information. We will take all reasonable steps to confirm your identity before making changes to Personal Information we may hold about you. We would appreciate it if you would take the necessary steps to keep your Personal Information accurate and up-to-date by notifying us of any changes we need to be aware of.

Security of Personal Information
We are legally obliged to provide adequate protection for the Personal Information we hold and to stop unauthorised access and use of personal information. We will, on an on-going basis, continue to review our security controls and related processes to ensure that your Personal Information is secure.

Our security policies and procedures cover:

Physical security;

- Computer and network security;
- Access to personal information;
- Secure communications;
- Security in contracting out activities or functions;
- Retention and disposal of information;
- Acceptable usage of personal information;
- Governance and regulatory issues;
- Monitoring access and usage of private information;
- Investigating and reacting to security incidents.

When we contract with third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that Personal Information that we remain responsible for, is kept secure.

We will ensure that anyone to whom we pass your Personal Information agrees to treat your information with the same level of protection as we are obliged to.

The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

Access to Personal Information

You have the right to request a copy of the Personal Information we hold about you. To do this, simply contact us at the numbers/addresses listed on our home page and specify what information you would like. We will take all reasonable steps to confirm your identity before providing details of your personal information.

Please note that any such access request may be subject to a payment of a legally allowable fee, as laid down in our POPI Act Policy.

Third Party Obligations

Service Providers have access to your Personal Information only to perform their tasks on our behalf and are obligated not to disclose or use it for any other purpose.

Service Providers

We may use Third-party Service Providers to provide better improvement of our Service.

Google Places

Google Places is a service that returns information about places using HTTP requests. It is operated by Google.

Google Places service may collect information from you and from your Device for security purposes.

The information gathered by Google Places is held in accordance with the Privacy Policy of Google: https://www.google.com/intl/en/policies/privacy/

Children's Privacy

Our Service does not address anyone under the age of 18. We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your child has provided us with Personal Information, please contact us. If we become aware that we have collected Personal Information from anyone under the age of 18 without verification of parental consent, we take steps to remove that information from our servers.

If we need to rely on consent as a legal basis for processing your information and your country requires consent from a parent, we may require your parent's consent before we collect and use that information.

Links to Other websites

Our Service may contain links to other websites that are not operated by us. If you click on a Third party link, you will be directed to that Third party's site. we strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any Third party sites or services.

Changes to this Privacy Notice

We may update our Privacy Notice from time to time. The notice currently in effect will be the one published on our Service and will contain the “Last Updated” date.

We will let you know via email and/or a prominent notice on our Service prior to updates but you are nevertheless advised to review the Privacy Notice periodically for any changes.

Contact us

If you have any questions about this Privacy Notice, you can contact us:

By email: compliance@cib.co.za

Annexure B

CCTV Camera Policy

1. INTRODUCTION

For the purpose of office security CIB installed a closed-circuit television ("CCTV") system. The cameras are positioned so that they record in and around the CIB office. Footage of these areas is recorded and stored for a limited amount of time. CIB undertakes to ensure that its employees, directors, affiliates, partners and/or clients adhere to the strictest levels of confidentiality and respect individual's right of privacy.

2. ACCOUNTABILITY

CIB "processes" "Personal Information" (which contained in the CCTV surveillance footage) as contemplated in the Protection of Personal Information Act, No. 4 of 2013 (the "Act"), always considering individual's constitutional right to privacy. The authorisation for the collection, location and access of the CCTV surveillance footage ("Data") lies with CIB. The Data may then be accessed through CIB's systems.

CIB is the party responsible for "processing" the Data, CIB is acting in the capacity of a "Responsible Party", as defined in the Act. CIB shall fully comply with its obligations in terms of the Act, depending on the capacity in which it is acting any given circumstance. CIB will be processing Personal Information where, given the purpose for which it is processed, such processing is adequate, relevant and not excessive. Details and records of all information processed by CIB will be maintained to the extent required by law.

3. PURPOSE

The purpose of this policy is to outline CIB's approach to the use of CCTV surveillance for purposes in line with the Act. Specifically, CIB strives to:

- process any Data lawfully, and in reasonable manner which does not unreasonably infringe on the privacy of the data subject;
- only process Data where, to do so, protects a legitimate interest of staff and members of the public;
- ensure each individual's constitutional right to privacy, by safeguarding Personal Information when processed by it or any of its customers (each of which constitutes a Responsible Party in terms of the Act), subject to justifiable limitations;
- balance the privacy rights of individuals against other rights, particularly the rights of members of staff and the general public to safety and security;
- regulate the way Data may be processed, by establishing conditions in accordance with locally applicable laws and international standards, that prescribe the minimum threshold requirements for the lawful processing of Personal Information;

- advise individuals of their rights and remedies in order to protect their Personal Information from processing that is not in accordance with the Act; and
- comply with voluntary and compulsory measures, including those established by the Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by the Act.

The purpose of CIB's CCTV surveillance network is to:

- detect, deter and prevent crime;
- enhance safety of those who work and visit the office areas covered by the CCTV surveillance network;
- assist in the apprehension and prosecution of offenders (including but not limited to the use of images and video as evidence in criminal/civil proceedings);
- assist law enforcement agencies, including private armed response and security companies, about the investigation of any apparent or actual crime that may be captured by the CCTV surveillance network;
- promote the safety, protection and wellbeing of staff and visiting members of the public.

Data gathered by the CCTV surveillance network will not be used for any purposes other than those listed above and/or permitted by the Act.

Data will not, under any circumstances, be released to the media or any similar outlet, nor will any Data be released or disseminated unless specifically required or authorised by law.

6. SCOPE AND OPERATION

CIB's CCTV surveillance network employs fixed cameras, designed and deployed to record images of individuals in and around the CIB office.

The CCTV surveillance network will be operated, and Data will only be made available, consistent with the requirements and restrictions imposed by the Act, always considering each individual's right to privacy.

All Data recorded on the CCTV network shall be reviewed by the Executive when necessary for the purpose of assisting with the identification and prevention criminal activity and in the interests of staff and the public's safety and security. All Data will be stored on servers. The Data will be stored for a period of at least 30 days, being the length of time, the Data is required to be maintained in order to achieve the purpose for which it was collected. This retention period may be increased or decreased in line with any lawful instruction provided by the Information Regulator or other competent authority from time to time. Data may be stored for a longer period should it be required for further investigation. At the expiry of this retention period, the data will be permanently deleted and/or destroyed in accordance with the Act's stipulated guidelines.

4. AWARENESS OF CCTV SURVEILLANCE

In order to ensure that all members of the public and staff entering any area in which the CCTV surveillance network operates are informed of the surveillance, prominent signs will be posted in these areas. Staff will also be reminded during employment.

5. RETENTION OF DATA AND SECURITY OF DATA

Data will be retained for up to 30 days, unless it is required and requested for purposes outlined in this policy which would require that the data be stored for a longer period. Appropriate safeguards will be put in place should such Data be retained for longer periods, as required by the Act.
Data retained for purposes of investigation will be strictly managed with limited access. Any Data requested by the South African Police Services will only be released upon presentation of the appropriate subpoena. All Data will be stored on secure servers owned by CIB.

After a period of 30 days (or such longer period as may be required per the above), the Data will be permanently erased and/or destroyed.

6. ACCESS TO CCTV SURVEILLANCE DATA BY CIB/CONTRACTED COMPANIES

Only specific persons within CIB will have the ability to access and review Data recorded by the CCTV surveillance network, and then only on a "need to know" basis.

These individuals include, from time to time:

- the CEO of CIB;
- the Managing Director of CIB;
- the CFO of CIB;
- the CIO of CIB;
- the Executive of CIB;
- the Information Officer of CIB;
- employees who are required to support or maintain the system;

The Information Officer, or other designated officer, will have the following responsibilities:

- conduct an annual review of CCTV surveillance network and usage;
- ensure that CCTV images are being stored securely and handled in accordance with this policy, the Act and all applicable laws;
- ensure that images are properly retained and stored, and that all electronic records are managed as any sensitive personal record would be within the CIB organisation;
- ensure that Data is disposed of in the manner required by the Act;
- ensure that any Data which is stored on any external storage system is securely encrypted;
- ensure access protocols are in place and are being followed by all personnel with access to any Data;
- ensure that viewing and disclosure of images is in line with CIB policy and legal obligations;

- ensure that staff using or maintaining the CCTV systems are sufficiently trained and aware of their obligations under the Act and any other applicable laws;
- ensure that each system is regularly maintained and identify if system upgrades are necessary; and
- ensure that each passive CCTV system has adequate signage advising members of the public and staff that they are being monitored.

Any unlawful disclosure of any Data, or any breach of any provision of the Act or any contract, shall be immediately addressed and, to the extent necessary, the breach will be reported to the Information Regulator, together with all details relating to the breach, as required in terms of the Act.

7. ACCESS TO DATA BY PRIVATE INDIVIDUALS

Individuals have the right to access Data of themselves in terms of the Act. Individuals may request that the relevant responsible party confirm, free of charge, whether the individual has been recorded on the CCTV network.

Individuals who have concerns over a potential infringement of their privacy may request a review of camera operations by contacting the parties responsible for monitoring the Data.

The requests for access to Data must include:

- exact date and time the images were recorded;
- information to identify the individual (if necessary);
- proof of identity; and
- location/area of the CCTV camera presumed to have recorded the Data;
- The party responsible for monitoring the Data in question shall promptly respond to the request.

In accordance with the Act, the party responsible for monitoring the Data in question may provide a record or a description of the Data that it has in its possession. A downloadable copy of the Data shall only be provided if, in the opinion of the responsible party, the Data requested does not contain personal information of anyone other than the requesting party and/or will be maintained safe and secure.

A reasonable fee will be charged for access to the Data, which fee shall be determined with reference to the time, technical expertise and resources which are required to expended on retrieving the Data and, where necessary, sanitising and de-identifying the Data to ensure no third-party rights are affected. The requesting party will be provided with a quotation for this fee as required by the Act.

If CIB cannot comply with the request, reasons shall be documented. The individual shall be advised of the reasons in writing, where possible.

Data will only be disclosed to third parties (being parties other than those acting on behalf of contracted companies or private individuals on their own behalf) if subpoenaed to do so, or otherwise compelled by law.

Access to the Data will only be released to third parties in terms of the Act or in terms of the Promotion of Access to Information Act ("PAIA"). Whichever may be applicable.

8. INFORMATION REGULATOR

In terms of the Act, the Information Regulator has been established and will be endowed with various power and authority once the Act is in effect.

The Information Regulator will, amongst other things, seek to provide education on the collection and use of personal information, monitor and enforce compliance with the Act, handle complaints, conduct research, assist with the preparation of sectoral codes of conduct and generally assist with the implementation of the Act and assist the general public on information related issues, where required. Any complaint in respect of any Data processed by CIB and/or its related security companies may be referred to the Information Regulator in writing at inforeg@justice.gov.za Additional information can be viewed at http://justice.gov.za/inforeg

Annexure C

Password Policy

Enforce Password History
This sets how frequently old passwords can be reused. With this policy, you can discourage users from alternating between several common passwords.

Maximum Password Age
This determines how long users can keep a password before they have to change it. The aim is to force users to change their passwords periodically. Generally, you use a shorter period when security is very important and a longer period when security is less important. You can set the maximum password age to any value from 0 to 999, where a value of 0 specifies that passwords don't expire. Although you might be tempted to set no expiration date, users should change passwords regularly to ensure the network's security. Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days.

Minimum Password Age
This determines how long users must keep a password before they can change it. You can use this field to prevent users from bypassing the password system by entering a new password and then changing it right back to the old one. If the minimum password age is set to 0, users can change their passwords immediately. To prevent this, set a specific minimum age. Reasonable settings are from three to seven days. In this way you make sure that users are less inclined to switch back to an old password but are able to change their passwords in a reasonable amount of time if they want to.

Minimum Password Length
This sets the minimum number of characters for a password. If you haven't changed the default setting, you should do so immediately. The default in some cases is to allow empty passwords (passwords with zero characters), which is definitely not a good idea. For security reasons you'll generally want passwords of at least eight characters because long passwords are usually harder to crack than short ones. If you want greater security, set the minimum password length to 14 characters.

Passwords Must Meet Complexity Requirements
On a basic level it should include:

- Passwords must have at least six characters.
- Passwords can't contain the username or parts of the user's full name, such as his first name.
- Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

- Passwords will be rotated every 30 days and the new password can’t be one of 15 previous passwords.

Store Password Using Reversible Encryption For All Users

Passwords in the password database are encrypted. This encryption can’t normally be reversed. The only time you would want to change this setting is when your organization uses applications that need to read the password. If this is the case, enable Store Password Using Reversible Encryption For All Users. But with this policy enabled, passwords might as well be stored as plain text—it presents the same security risks. With this in mind, a much better technique is to enable the option on a per-user basis and then only as required to meet the user’s actual needs.

Annexure D

Bring Your Own Device Policy

CIB (Pty) Ltd: BYOD Policy

CIB (Pty) Ltd ("CIB") allows the relevant employees to use smartphones and tablets of their choosing at work for their convenience when required. CIB reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

As part of your overall POPI Act compliance risk assessment to comply with Condition 7 (Security Safeguards, Section 19), This policy is intended to protect the security and integrity of CIB's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

CIB employees must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network.

Acceptable Use

The company defines acceptable business use as activities that directly or indirectly support the business of CIB.

The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.

Devices connected to the company's network may not be used at any time to:

- Store or transmit illicit materials.
- Store or transmit proprietary information belonging to another company.
- Harass others.
- Engage in outside business activities.

Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents at the discretion of the company this is subject to change from time to time. Employees to be careful of untrusted connections, for example open Wi-Fi networks in coffee shops, hotels, and shopping centres etc.

Device(s) means devices that have components for controlling the flow of electrical currents for the purpose of information processing and system control.

Security

To prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the company network.

Company Email Passwords must be at least 12 characters and a combination of upper- and lower-case letters, 2 numbers and symbols. Passwords will be rotated every 30 days and the new password cannot be one of 5 previous passwords.

The device must lock itself with a password or PIN if it is idle for one minute.

Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

The employee's device may be remotely wiped in respect of Company data only if 1) the device is lost, 2) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device in respect of Company data only, it is the employee's responsibility to take additional precautions, such as backing up personal email, contacts, etc. Intune applications and operating system to be kept always updated. The employee indemnifies the Company from any loss/risk during wiping or removing of company data from the personal device. The Intune application will only remove software that has been inventoried by CIB.

End of employment contract – All access to apps used for company purposes will be revoked. All data on these applications will be wiped remotely.

The company reserves the right to disable company email services.

Lost or stolen devices must be reported to IT immediately via the helpdesk and direct line manager to be notified. Employees are responsible for notifying their cellular/mobile service provider immediately upon loss of a device.

The employee is always expected to use his or her devices in an ethical manner and adhere to the company's acceptable use policy as outlined above.

The employee is personally liable for all costs associated with his or her device.

CIB reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Annexure E

Personal Information Sharing Policy

During the normal course of business CIB may disclose a client's personal information to its subsidiary, the insurer underwriting the portfolio, reinsurers or third-party service providers. CIB has agreements in place to ensure that compliance with the relevant legislation is adhered to. CIB may also share client personal information with and obtain information about clients from third parties for the reasons already mentioned. CIB may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect CIB rights.

Annexure F

Printing Policy

Where data is stored on paper, it will always be kept in a secure place where an unauthorised person cannot access or see it. This also applies to data stored electronically which has been printed out for some reason.

When not required such papers should be kept in a locked drawer, safe or cabinet.

Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g., on a printer, and all unwanted paper must be shredded by disposing of it in the designated bins.

Annexure G

Subject Access Request Policy

Where an employee or individual who is entitled to it contacts the company requesting his/her personal information, it is called a “subject access request”.

Employees and individuals who are the subject of personal data held by CIB are entitled to:

- enquire what information is held about them and the purpose for holding it;
- enquire how to gain access to their own personal data;
- be informed of any special measures the company uses to keep such data up to date.

Subject Access Requests shall be made by e-mail and addressed to the Deputy Information Officer who shall address it in consultation with management.

The identity of a person making a data subject request will always be verified before handing over any information requested.

Annexure H

Data Protection Policy

1. Introduction

CIB is an underwriting manager and an authorised financial services provider.

Inherent in the provision of these services to its clients, as well as the management of its employment relationships with its own "employees" (both permanent and on various types of contracts), CIB continually has access to and needs to process personal data and information relating to individuals.

This policy sets out how such personal data shall be processed and to comply with the legal standards governing its clients as well as future legislation which may be enacted into law in South Africa in the foreseeable future.

This Data Protection Policy seeks to ensure that CIB:

- Complies with legal standards and best practice for the receipt, importing, processing, handling and storing of personal data of individuals ("data subjects"), both as received from its clients, and as held in respect of its own employees;

- Protects the rights of its own employees, as well as that of its clients and third parties in respect of individuals' data;

- Transparently renders how it process, handles and stores individuals' data;

- Protects itself from the risks of a data breach.

2. Legislative Environment

This policy seeks to align best practice in CIB with legal standards governing its clients, including the Protection of Personal Information Act ("POPI").

In doing so, it is acknowledged that CIB receives and/or imports data from brokers and/or clients to enable CIB to provide services. CIB does however, collect or gather data from its own employees for various purposes related to human resources and employment benefit administration.

3. Scope and Application

This policy applies to all employees of CIB in respect of all personal data accessed in the provision of services by CIB to its clients, as well as the management of its employment relationships with its own employees.

It further applies to all data that it holds relating to identifiable individuals, including, but not limited to the following:

names of individuals; physical addresses; postal addresses; email details; all telephone and mobile phone numbers; identifiers; absolutely all data and information relating to an individual received from a broker or client in the course of providing services to such client, and/or all data of a data subject protected for the benefit of such individual in terms of POPI or sought to be protected by the latter statute.

4. Protection

This policy seeks to protect CIB from various very real data security risks including;

Breaches of confidentiality through data breaches, hacking risks, and the risks of liability in relation to its clients, third parties data acquired from such clients and all its own employees.

The rules and standards set out in this policy applies regardless of –

• whether personal data relates to a client or an employee of CIB, and/or

• is stored electronically, digitally, on paper, or on other materials, or through other methods.

5. General rules relating to Personal Data

Personal data shall at all times be:

- processed fairly and lawfully, in accordance with legal standards applicable to such data or data categories;

- obtained only for specific lawful purposes;

- adequate, relevant and not excessive;

- accurate, and kept up to date;

- held for no longer than necessary for the purpose it was obtained for;

- processed in accordance with the rights of data subjects;

- be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically;

- not be disclosed or transferred or exported illegally, or in breach of any agreement with a client.

6. Responsible Parties

All employees shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of data personal data in the execution of employment duties and services to CIB, or otherwise in the course of rendering services or being associated with the company.

7. The Information Officer

The Information Officer shall –

- in time be registered as the responsible officer under POPI, once enacted in South Africa;

- execute, and bear responsibility for reporting to executive management about compliance with all technological and operational data protection standards and protocols and advise of any risk of breach at the earliest opportunity with a view to avoiding any risk or breach, or limiting any damage resulting from it. To ensure compliance with this provision, a Breach Notification Form must be completed by any employee of CIB who becomes aware of any breach /or possible breach;

- ensure that all operational and technological data protection standards are complied with;

- arrange data protection training and provide advice and guidance to all employees;

-be entitled and have authorisation to initiate disciplinary proceedings against any employee who at any time breaches any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) ("rule") applicable in any department or area of the operations of the company;

- review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;

- attend to requests from individuals to access data CIB holds about them "data subject requests".

8. The CIO (External IT Service Provider)

The CIO shall –

- ensure that all systems services and equipment used for processing and/or storing data adhere to acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;

- issue appropriate, clear, regular rules and directives, whether for the organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the company's work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sing-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.

- evaluate any third-party services the company is considering or may acquire to process or store data, e.g. cloud computing services.

Note: It is acknowledged that these rules, directives and protocols are in themselves operationally confidential and to the company and organisation and may be adjusted or changed at any time whether verbally or otherwise for a particular individual or group of individuals or the company as a whole, in order to ensure an adaptive, responsive, efficient functional IT management system which serves the requirements and risks of CIB and all its clients and employees. For this reason, it is confirmed that not all such rules, directives and protocols will be captured in writing, as it may undermine or impair the afforested goals, if should this be the case.

9. General Data Protection Rules

All personal data shall be deemed confidential information and be handled as such.

The only person/s entitled to access data covered by this policy, will be those who need to access it for the execution of their direct work services or required outputs.

Under no circumstances will data or personal information be shared outside the scope of required work outputs, or informally. In the event of any doubt, an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary.

Employees will receive induction and on-the-job training in relation to all security standards applicable to such employee's service delivery and work outputs involving personal information of data subjects.

Employees shall keep all data secure by taking sensible practical precautions and complying with all rules, practices and protocols:

- In particular, strong passwords shall be used at all times;

- Passwords shall not be shared under any circumstances;

Note: In the exceptional circumstance that a password may require to be shared, it shall only take place after explicit, provable authorisation has been procured from a senior manager or line manager before sharing it, and then only for the stated purpose. All necessary steps shall be taken after a password has been shared in such exceptional circumstances, to reset it to a strong, unique password to avoid future data compromise or breach.

10. Data Storage

10.1. Paper

Where data is stored on paper, it will always be kept in a secure place where an unauthorised person cannot access or see it. This also applies to data stored electronically which has been printed out for some reason.

When not required by such papers should be kept in a locked drawer, safe or cabinet.

Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g., on a printer, and all unwanted paper must be shredded by disposing of it in the allocated bins.

10.2. Electronic data

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;

- Where data is stored on removable media such as a CD or a DVD these must at all times be locked away securely when not in immediate use;

- All data will only be stored on designated drives and servers and shall only be uploaded to approved cloud computing services;

- All servers containing personal data will be located in secure protected locations away from general office space;

- Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the CIO. The Information Officer will be responsible to schedule a minimum of two random tests each year;

- Data will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;

- All servers and computers containing data will be protected by approved security software, and one or more firewalls under the direction of the CIO.

11. Data Use

It is acknowledged that personal data is at the greatest risk of loss, breach of confidentiality, corruption, hacking or theft when it is accessed or used. Therefore, when working with personal data, employees should ensure that screens of their computers are always locked when left unattended;

Personal data will not be shared informally, and in particular it will never be sent by email or without protection with appropriate passwords, where required to be sent by email;

Data shall be encrypted before being transferred electronically. The CIO together with the Information Officer will develop and maintain protocols for data transfer to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties;

Personal data shall never be transferred or sent to any entity not authorised directly to receive it;

Employees are prohibited from saving copies of personal data to their own computers;

Employees will at all times access and update only the central, official copy of any data or work output document, such as payroll.

Personal data is not of value to CIB, unless the business makes use of it in the course of providing services to its clients or administering its own employment relationships with employees.

12. Data Accuracy

Employees shall take reasonable steps to comply with company rules and work practices to ensure data is kept accurate and up to date;

The more important the accuracy of any component of personal data is, the greater the effort and measures will be to ensure its accuracy;

Data will always be held in as few places as necessary to ensure efficient service delivery and risk avoidance. Employees are not permitted to create any unnecessary additional data sets;

Employees will make use of every opportunity to ensure that a data component is accurate and up to date, e.g. by confirming details when handling a client call.

Employees shall at all times remain knowledgeable and informed about all data updating practices and work protocols used by CIB, such as updating via official, acknowledged websites and platforms used by clients.

13. Data Subject Access Requests

Where an employee or individual who is entitled to it contacts the company requesting his/her personal information, it is called a "subject access request".

Employees and individuals who are the subject of personal data held by CIB are entitled to:

- enquire what information is held about them and the purpose for holding it;

- enquire how to gain access to their own personal data;

- be informed of any special measures the company uses to keep such data up to date.

Subject Access Requests shall be made by e-mail and addressed to the Information Officer who shall address it in consultation with management.

The identity of a person making a data subject request will always be verified before handing over any information requested.

14. Providing Information

In certain circumstances, South African legislation will allow that personal data be disclosed to law enforcement or other agencies without the consent of the data subject. In such circumstance, CIB may be obliged to disclose the requested data, but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers or other experts. Only the Risk and Compliance Officer will be authorised to furnish the requested data to the enquiring party.

15. Disciplinary Code and Incorporation of this Policy into the Employee's Employment Contract

This data protection policy governs every employee of CIB, both during the course of his/her services to it, and to the extent applicable, after termination of services.

To the extent that this policy sets out workplace rules (as defined) governing the employee in the course of his/her work and services to the company, it shall form part of the company's Disciplinary Code and Procedure and is hereby also incorporated into it.

A breach of any rule in relation to the protection of personal data set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal.

The imposition of any disciplinary sanction or dismissal shall not preclude the company from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations.

[Note: It shall be incumbent upon every employee to familiarise him/herself with the content of this policy, and to remain up to date as to any changes to it issued in written form as part hereof by the company.]

Annexure I

Security Compromises Policy

1. Protection of Personal Information Act

In the event of a security compromise, CIB will notify the Information Regulator as well as any parties whose personal information have been accessed or acquired by an unauthorised party.

The notification must contain the following information:

- A description of the possible consequences of the security compromise;
- A description of the measures taken or proposed to be taken by the responsible party to remedy the security breach;
- A recommendation of the measures that any party whose personal information was leaked in the security compromise should take in order to mitigate the possible adverse effects of the security compromise;
- The identity of the unauthorised person, if known, who accessed or acquired the personal information.

Should the Information Regulator require the data breach to be publicised it will be published accordingly.

2. General Data Protection Regulation (GDPR)

If the personal information of individuals in the European Union (EU) is affected by a data breach in South Africa, CIB will notify the supervisory authority in the EU without undue delay, and at the latest within seventy-two hours after having become aware of the security breach.

The notification in this case must:

- Describe the nature of the breach;
- State the categories and number of persons affected by the breach;
- State the contact details of the data protection officer where further information can be obtained;
- Describe the likely consequences of the breach; and
- Describe the measures taken or proposed to be taken by the Company to remedy the breach, including measures to mitigate its possible adverse effects.

Annexure J

Cookie Policy

This Cookies Policy explains what Cookies are and how We use them. You should read this policy so You can understand what type of cookies We use, or the information We collect using Cookies and how that information is used. Our Cookies Policy is maintained by the Cookies Policy Generator.

Cookies do not typically contain any information that personally identifies a user, but personal information that we store about You may be linked to the information stored in and obtained from Cookies. For further information on how We use, store and keep your personal data secure, see our Privacy Policy.

We do not store sensitive personal information, such as mailing addresses, account passwords, etc. in the Cookies We use.

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions.

The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Cookies Policy:

Company (referred to as either "the Company", "We", "Us" or "Our" in this Cookies Policy) refers to CIB (Pty) Ltd, Riley Road 15E.

You means the individual accessing or using the Website, or a company, or any legal entity on behalf of which such individual is accessing or using the Website, as applicable.

Cookies means small files that are placed on Your computer, mobile device or any other device by a website, containing details of your browsing history on that website among its many uses.

Website refers to CIB, accessible from https://www.cib.co.za/

The use of the Cookies

Type of Cookies We Use

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close your web browser.

We use both session and persistent Cookies for the purposes set out below:

Necessary / Essential Cookies

Type: Session Cookies

Administered by: Us

Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

Functionality Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

Your Choices Regarding Cookies

If You prefer to avoid the use of Cookies on the Website, first You must disable the use of Cookies in your browser and then delete the Cookies saved in your browser associated with this website. You may use this option for preventing the use of Cookies at any time.

If You do not accept Our Cookies, You may experience some inconvenience in your use of the Website and some features may not function properly.

If You'd like to delete Cookies or instruct your web browser to delete or refuse Cookies, please visit the help pages of your web browser.

For the Chrome web browser, please visit this page from Google:
https://support.google.com/accounts/answer/32050

For the Internet Explorer web browser, please visit this page from Microsoft:
http://support.microsoft.com/kb/278835

For the Firefox web browser, please visit this page from Mozilla: https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored

For the Safari web browser, please visit this page from Apple:
https://support.apple.com/guide/safari/manage-cookies-and-website-data-sfri11471/mac

For any other web browser, please visit your web browser's official web pages.

Contact Us

If you have any questions about this Cookies Policy, You can contact us:

By email: compliance@cib.co.za

Annexure K

Record Retention Policy

Index

Annexure 1

1. Policy and Purpose

To ensure the most efficient and effective operation of CIB (Pty) Ltd ("The Company"), we are implementing this Document Retention Policy ("DRP" or "policy"). The records of The Company are important to the proper functioning of The Company. Our records include virtually all of the records produced by the staff of the Company. Such records can be in electronic or paper form. Notwithstanding the foregoing, the Company reserves the right to revise or revoke this Policy at any time.

2. The goals of this DRP are to:

2.1. Retain important documents for reference and future use;
2.2. Dispose of documents that are no longer necessary for the proper functioning of the Company;
2.3. Organise important documents for efficient retrieval;
2.4. Ensure that The Company employees know what documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed;
2.5. Compliance with the Protection of Personal Information Act 4 of 2013.

3. Reason for the DRP

SARS and The Company's Act require The Company to maintain certain types of records for particular periods. Failure to maintain such records could subject the Company to penalties and fines, obstruct justice, spoil legal evidence, and/or seriously harm The Company's position in litigation. Thus, it is imperative that staff fully understand and comply with this, and any future records retention or destruction policies and schedules.

4. What is classified as records?

"Records" discussed herein refers to all business records of The Company and personal information of policyholders and employees (and is used interchangeably with "documents"), including written, printed, and recorded materials, as well as electronic records (i.e., emails and documents saved electronically). All business records shall be retained for a period no longer than necessary for the proper conduct and functioning of The Company.

5. Document retention

Refer to annexure A for details on retention periods for different categories of records.

6. **Electronic Documents; Document Integrity**.

Documents in electronic format shall be maintained just as hard copy or paper documents are, in accordance with the Document Retention Schedule. Due to the fact that the integrity of electronic documents, whether with respect to the ease of alteration or deletion, or otherwise, may come into question, the Administrator shall attempt to establish standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents, and regular check-ups of the reliability of the system; provided, that such standards shall only be implemented to the extent that they are reasonably attainable considering the resources and other priorities of the Company.

7. Emergency Planning.

Documents shall be stored in a safe and accessible manner. Documents which are necessary for the continued operation of the Company in the case of an emergency shall be regularly duplicated or backed up and maintained in an off-site location. The Administrator shall develop reasonable procedures for document retention in the case of an emergency.

Annexure 1

1. The Companies Act

The Companies Act, No 71 of 2008, consolidates and amends the law that relates to companies. This Act became effective on 1 May 2011 and should be read with the Companies Amendment Act, No 3 of 2011, and the Companies Regulations, 2011.

The Act expressly provides that records must be kept "in written form, or other form or manner that allows that information to be converted into written form within a reasonable time".

	Document	**Retention period**
	Reference: Section 24	
11.1.	General rule for company records: Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act and other public regulation	7 years or longer (as specified in other public regulation)
11.2.	Registration certificate	Indefinite
11.3.	Memorandum of Incorporation and alterations or amendments	Indefinite
11.4.	Rules	Indefinite
11.5.	Securities register and uncertificated securities register	Indefinite

11.6.	Register of company secretary and auditors	Indefinite
11.7.	Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) - Register of disclosures of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued	Indefinite
11.8.	Notice and minutes of all shareholders meeting including: - Resolutions adopted - Document made available to holders of securities	7 years
11.9.	Copies of reports presented at the annual general meeting of the company	7 years
11.10.	Copies of annual financial statements required by the Act	7 years
11.11.	Copies of accounting records as required by the Act	7 years
11.12.	Record of directors and past directors, after the director has retired from the company	7 years
11.13.	Written communication to holders of securities	7 years
11.14.	Minutes and resolutions of directors' meetings, audit committee and directors' committees	7 years

2. Labour Relations

Employee relations are governed by a variety of legislation, including the Basic Conditions of Employment Act and the Labour Relations Act. The Basic Conditions of Employment Act No. 75 of 1997 states that various documents relating to employees should be kept for future reference:

	Document	**Retention Period**
2.1	Written particulars of employee must be kept after termination of employment.	3 years
2.2	Employee's name and occupation	3 years
2.3	Time worked by each employee	3 years
2.4	Remuneration paid to each employee	3 years
2.5	Date of birth of any employee under 18 years of age	3 years

3. Health and Safety

The Compensation for Occupational Injuries and Diseases Act No. 130 of 1993 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 by these injuries at their place of work.

The Act states that certain records should be retained:

	Document	**Retention Period**
3.1	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees	4 years

4. Taxation

The Income Tax Act No. 58 of 1962 is the act governing all the laws relating to income taxes and donations and the Value Added Tax Act No. 89 0f 1991 provides for the taxation of the supply of goods and services as well as the importation of goods and services. These acts provide specific time periods that documents must be retained:

	Document	**Retention Period**
	Income tax	

4.1	Records kept by person who has rendered a return (from date return was lodged) including:	5 years
	- ledgers	
	- cash books	
	- journals	
	- cheque books	
	- bank statements	
	- deposit slips	
	- paid cheques	
	- invoices	
	- other books of accounts	
	- electronic representations of information	
4.2	Records relating to taxable capital gain or assessed capital loss (from date return was lodged):	5 years (But the CIB policy is to retain these documents **Indefinitely**)
	- agreement for acquisition, disposal or lease of asset	
	- details of asset transferred into a trust	
	- copies of valuations used in determining the taxable capital gain or assessed capital loss	
	- invoices or other evidence of payment records such as bank statements and paid cheques relating to any costs claimed in respect of the acquisition, improvement or disposal of any asset	
	- details supporting the proportional use of an asset for both private and business purposes	
	- details of any continuous absence of more than6 months from a primary residence, as contemplated in the Eighth Schedule	
4.3	Documents relating to where objection and appeal is lodged Until	appeal/objection is finalised
	Value added tax	
4.4	Vendors are obliged to keep the following records (from date the income tax return was lodged):	5 years
	- Record of all goods and services	
	- the rate of tax applicable to the supply and the suppliers or their agents	
	- invoices	
	- tax invoices	
	- Credit notes	
	- Debit notes	
	- bank statements	
	- deposit slips	
	- paid cheques	

4.5	Vendors should keep the following information:	5 years
	- charts and codes of accounts	
	- accounting instruction manual	
	- system and programme documentation which describes the accounting system used in the various accounting period	
	- where the vendor's basis of accounting has changed lists of debtors and creditors as at the end of the tax period immediately preceding the changeover period	
4.6	Documentary proof substantiating the zero rating of supplies	5 years

The documents relating to Income Tax must be retained in their original form or electronic format as prescribed by the Commissioner. The documents relating to VAT shall be kept in either a book form for a period of 5 years after the completion of the last entry in the book or in another form for a period of 5 years
after the completion of the last transactions, acts or operations to which they relate. The Commissioner may determine the form in which information may be kept including electronic format. This does not however apply to original record of ledgers, cash books, journals and paid cheques.

5. Electronic Communication and documents

The Electronic Communication and Transaction Act, No 25 of 2005, regulates electronic communication and prohibits the abuse of information. Certain principles are stated for the electronic collection of personal information and also the timeframe in which this information must be kept:

	Document	**Retention period**
	Reference: Section 51	
1.1.	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information	As long as information is used, and at least 1 year thereafter
1.2.	A record of any third party to whom the information was disclosed must be kept for as long as the information is used	As long as information is used and at least 1 year thereafter
1.3.	All personal data which has become obsolete	Destroy

6. Financial Advisory and Intermediary Services Act, No 37 of 2002

The Financial Advisory and Intermediary Services Act, No 37 of 2002, seeks to regulate the rendering of certain financial advisory and intermediary services to clients and to provide for matters incidental to these services.

	Document	**Retention period**
	Reference: Section 18	

1.1.	An authorised financial services provider must maintain the following records regarding- - known premature cancellations of transactions or financial products by clients of the provider; - complaints received together with an indication whether or not any such complaint has been resolved; - the continued compliance with the requirements referred to in section 8; - cases of non-compliance with this Act, and the reasons for such non-compliance; and - the continued compliance by representatives with the requirements referred to in section 13(1) and (2) .	5 years (except to the extent exempted by the registrar)
	General Code Of Conduct For Authorised Financial Services Provider And Representatives Section 3	
1.2.	Specific duties of provider A provider must have appropriate procedures and systems in place to- - record such verbal and written communications relating to a financial service rendered to a client as are contemplated in the Act, this Code or any other Code drafted in terms of section 15 of the Act; - store and retrieve such records and any other material documentation relating to the client or financial service rendered to the client; and - keep such client records and documentation safe from destruction. All such records must be kept for a period after termination, to the knowledge of the provider, of the product concerned or, in any other case, after the rendering of the financial service concerned. Providers are not required to keep the records themselves but must ensure that they are available for inspection within seven days of the registrar's request. Records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form.	5 years

7. Protection of Personal Information Act 4 of 2013

The purpose of the Protection of Personal Information Act 4 of 2013 is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information; and protecting important interests, including the free flow of information within the Republic and across international borders. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information and to provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and furthermore establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

	Document	**Retention period**
	Reference: Section 14	

1.1.	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person	(1) Records of personal information must not be retained any longer than necessary for achieving the purpose for which it was collected unless: (a) retention of the record is required or authorised by law; (b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities; (c) retention of the record is required by a contract between the parties thereto; or (d) the data subject or a competent person where the data subject is a child has consented to the retention of the record (2) Records of personal information may be retained for periods in excess of those contemplated in section 14 (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes. (3) A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must: (a) retain the record for such period as may be required or prescribed by law or a code of conduct; or (b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record. (4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of section 14 (1) or (2). (5) The destruction or deletion of a record of personal information in terms of section 14 (4) must be done in a manner that prevents its reconstruction in an intelligible form. (6) The responsible party must restrict processing of personal information if:

		(a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information; (b) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or (d) the data subject requests to transmit the personal data into another automated processing system. (7) Personal information referred to in section 14 (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest. (8) Where processing of personal information is restricted pursuant to section 14(6), the responsible party must inform the data subject before lifting the restriction on processing.

8**. The Employment Equity Act, No 55 of 1998**

The Employment Equity Act, No 55 of 1998, provides for employment equity and applies to employers and employees. The Act has certain requirements with regard to the retention of certain documents.

	Document	**Retention period**
	Reference: Section 26	
1.1.	An employer must establish and maintain records in respect of its workforce, its employment equity plan and other records relevant to compliance with the Act for the prescribed period.	
	General Administrative Regulations, 2009 Reference: Regulation 3(2)	
1.2.	A designated employer who employs 150 or more people must retain the employment equity plan.	3 years after expiry of plan
1.3.	A designated employer who employs fewer than 150 people must retain the employment equity plan.	2 years after expiry of plan
	Reference: Section 21 General Administrative Regulations, 2009 Reference: Regulation 4(10) and (11)	
1.4.	A designated employer must submit a report to the Director General as indicated in section 21. This report should be retained after submission to the Director General: - by a large employer	3 years

	- by a small employer	2 years

9. Unemployment Insurance Act, No 63 of 2002

The Unemployment Insurance Act, No 63 of 2002, applies to all employers and workers, but not to –

- Workers working less than 24 hours a month for an employer;
- Learners;
- Public servants;
- Foreigners working on contract;
- Workers who get a monthly State (old age) pension; or
- Workers who only earn commission.

Domestic employers and their workers have also been included under the scope of the Act since 1 April 2003.

	Document	**Retention period**
	Reference: Section 56(2) (c)	
1.1.	Employers must maintain personal records of each of their current employees in terms of - names; - identification numbers; - monthly remuneration; and - address where the employee is employed	Refer to section 14 of the Protection of Personal Information Act No. 4 of 2013 – records of personal information must not be retained any longer than necessary for achieving the purpose for which it was collected

Annexure L

IT Security Policy

Purpose

This policy document is intended to provide and set a policy for IT security in the CIB IT environment. This IT security policy is a formal statement of the rules that employees and others must follow when using this organisation's IT infrastructure.

The requirements and policies specified within this manual are extended to all CIB premises irrespective of the location.

This policy will ensure:

- A safe, productive and inoffensive work environment;
- Fair and equitable use of system resources by all authorised users;
- The maintenance and security of corporate information; and
- Compliance with legal and contractual obligations.

Scope

This policy applies to all:

- Employees
- Contractors
- Contracted organisations
- Vendors
- Agents
- Interns
- Consultants
- Employees of CIB subsidiaries, and
- Affiliates in which CIB is the single Shareholder or has defined management control
- Anyone that makes use of or is connected to the CIB IT environment.

Definitions

Term	Definition
CIB	CIB
"Business Day"	This refers to the time period between 8:00 AM and 17:00 PM, Mondays to Fridays, except for public holidays and announced closures
"Deployment"	Put IT Assets into use in an organised and planned manner
"IT"	Information Technology
"IT System"	An integrated combination of one or more processes, hardware components, software, facilities and people, that provides the capability to satisfy a stated business need or objective. It is a collection of resources and configuration items or assets that are necessary to deliver an IT Service.
"Information Management (IM)"	The information Management function of CIB and its operating entities

Policy Directives

Information is an important asset that enables and sustains the ability to do business. Since a significant proportion of the critical business functions are supported by IT systems and services, those systems and services must be protected in a cost effective manner according to the Availability, Integrity and Confidentiality requirements of the system and / or service.

- CIB requires all access to systems, devices, data and folders to be managed securely through an authorisation, authentication and review process.
- CIB IT infrastructure used or created by CIB resources are considered assets and property of CIB and must be used and protected as such.
- Usage of and access to CIB IT infrastructure and resources are provided to authorised users in support of the CIB business.
- IT services including desktop and software services may be provided either by CIB IT department or by other organisations as agreed by the Chief Information Officer.
- CIB IT reserves the right to access CIB's computer systems and data entrusted to authorised users at any time.
- CIB IT may at its discretion, with or without notice:
  - Examine electronic records, files, information or other data;
  - Monitor individual login sessions;
  - Remove / destroy files used for security attacks.
- Each user is responsible for any and all activity initiated in, on or from his/her user access account.
- Individual users must have their own user access account and select a secure password for that account and must keep their passwords secret at all times.
- No user is allowed to log onto a system / server with a service account to access information or perform any function, unless it is part of an authorised change request or to change a system account password to resolve an incident and this action must be logged in the incident record.
- Users must protect their own system files and data from being accessed by other users.
- Users are responsible for backup of data on their local hard drives.
- Users may not block efforts or ability by CIB IT department to collect information about CIB IT infrastructure and resources.
- As a general rule, users should delete e-mail received from an unknown person. Never reply to the sender of the e-mail. Never open an attachment to an e-mail unless the sender is known by the user and the attachment is expected.

Acceptable Usage

- Any operations that interfere with the normal running or performance of any of the CIB systems are not permitted.
- Any attempt to decrypt passwords or gain unauthorised access to CIB systems or data is not permitted, except where this is an authorised security review.
- Use of any CIB systems for personal gain is not permitted.
- Providing false or misleading information for purposes of obtaining access to CIB's IT infrastructure and resources is a violation of this policy.

Authentication and Authorisation

- All users are required to be authenticated on the CIB network before getting access to the various systems.
- It is the responsibility of the Business Unit managers or delegate to complete the required documentation (CIB User Request Form) to get a user domain, network or network point access. Only the Chief Information Officer or delegate can sign off access to domain, network or network point access.
- It is the responsibility of the requestor to complete the required documentation (CIB Access Request Form) to get access to resources and shares (including printers). Only the relevant owner or delegate can sign off the required access.
- It is the responsibility of the requestor to complete the required documentation (CIB Access Request Form) to get access to applications. Only the relevant owner or delegate can sign off required access.
- When completing the CIB User Request form, managers should also indicate what other IT resources the users should have access to, including but not limited to:
  - What distribution lists they should be added to;

- What applications and the roles within those applications the user should be given access to;
- What folders the users should be given access to.

- Authentication to the network will take place in terms of the CIB Password Policy.
- Users are not to share, write down, save in unencrypted files or documents or send via email their username and passwords in line with the CIB Password Policy.
- No one person will have full systems rights to any system.
- Network and server passwords, system and database passwords will be controlled by the Chief Information Officer.
- The Chief Information Officer will be responsible for determining end-user access rights to systems where queries / disputes arise.
- User rights will be granted as per Account Privileges Policy.
- Once IT Support has been advised that the user is no longer to have access, their network access will be disabled for a 30 day period, and thereafter the email account is archived / backed-up before deletion.
- Auditing will be implemented on all systems to record login attempts / failures, successful logins and changes made to all systems.
- Use of the Administrator and Service Accounts must be kept to a minimum and administrators must log onto systems using their own usernames. System automation must be setup to only use Service Accounts and not personal user names.
- File systems will have the maximum security implemented that is possible.
- Default passwords on systems must be changed after first login.
- Login and passwords must not be coded into programs or queries.

Contracts with third parties

- Contracts and Service Level Agreements with third parties and service providers must include security conditions.

Information classification

- The information created by and stored on CIB's information systems must be retained from a minimum period that meets both legal and business requirements.
- The archiving of electronic records, files, information or other data must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff.
- Any access to company records, files, information or other data contained on any database, or the use of such records, files or information when the authorised user has no job related need for such information is prohibited.

Access and use of corporate registries

- Access and use of corporate registries (examples include HR database, customer information, etc.) and associated local directories, are permitted only if the registry permits such access.
- Permission to access Corporate Registries is administrated by the business unit that owns the registry.
- With the exception of backup and recovery purposes, no corporate registry may be copied or distributed, in whole or in part, without prior permission and consent from the Chief Information Officer.

Personnel security

- Disciplinary measures against employees who deliberately or persistently behave in a way that is detrimental to security are defined in the *Employee Code of Ethics* document.
- Human Resources must ensure that all personnel with Internet access and / or e-mail are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet and / or e-mail in addition to compliance with CIB Information Security Policies.
- Upon notification of a staff resignation revoke all access rights. Upon specific request, CIB IT department will archive user data.
- Guidelines regarding access to and disclosure of electronic mail messages sent or received by CIB employees are contained in the Electronic Messaging Policy.

Network security

- The CIB network must be safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall.
- The organisation will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by staff. Management will, on a regular basis analyse reports of attempted access.
- Unless authorised by the Chief Information Officer, users from non-IT departments are prohibited from using CIB assigned internet IP addresses for any unauthorised purpose whatsoever.
- CIB IT is responsible for maintaining a log of those personnel who have administrative rights.
- No user may use CIB resources or network connections to make unauthorised connections to, break into, or adversely affect the performance of other systems or networks connected to the CIB network.
- Remote access to the organisation's network and resources will only be permitted provided that authorised users are authenticated and privileges are restricted.
- Third party access to corporate information is only permitted where the information in question has been 'ring-fenced' and the risk of possible unauthorised access is considered to be negligible.

Local area network (LAN) security

- LAN equipment, hubs, routers, switches will be kept in a secure location. The location access will be controlled by CIB IT.
- Users must log out of or lock their workstations when they leave their workstation for any length of time.
- The use of LAN analyser and packet sniffing software is restricted to the CIB IT Infrastructure team and approved auditors.
- Access Control must be managed by using Intrusion detection systems.
- Access to the system console and server disk/tape drives must be restricted to authorised CIB IT Infrastructure staff only.

Wide area network (WAN) security

- Users may not install their own wireless equipment under any circumstances.
- Dial-in modems may not be used, unless approved by the Chief Information Officer.
- A secure VPN tunnel must be used as the preferred WAN connection.
- All routers and gateways will be kept locked in a secure location.

Server specific security

- The operating system must be kept up to date and patched on a regular basis.
- Servers must be checked daily for viruses.
- Servers must be locked in the server room

Internet security

- Access to the internet and/or web is provided for legitimate business related activities.
- Downloading, possession, distribution or copying of copyright work is an infringement of copyright laws unless the person downloading it is authorised to do so by the copyright owner.
- All CIB connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk or confidential.

Cabling security

- Network cabling should be installed and maintained by the change control policy to ensure integrity of both the network and the wall-mounted sockets.
- Cables and plugs in secure locations should be properly secured to prevent someone accidentally disconnecting them.

Virus Protection

- Without exception, Anti-virus software must be deployed across all applicable workstations, mobile devices, servers and laptop computers with regular virus definition updates and scanning.

System Security

- All CIB systems connected to the Internet must have a vendor supported version of the operating system installed and must have the latest security patches loaded on them.
- Regular system integrity checks of host and server systems housing CIB confidential data must be performed.
- Access to certain systems must be logged and monitored to identify potential misuse of systems or information.
- Systems access must be monitored regularly to prevent attempts at unauthorised access and to confirm that access control standards are effective. Intrusion detection systems are to be used where the risk of intrusion is highest.
- Intrusion detection monitoring must be performed only on access from outside the CIB domain.
- Access to business applications must be authorised by the system owner.
- A user's access to business application(s) must be enabled by an authorised system administrator.
- All systems and software applications must offer the required level of security throughout their operational life.
- Software developed for or by CIB must always follow a formalised development process.
- No user may develop or use programs which:
  - Access resources that the user does not have authority to access;
  - Attempt to bypass system security mechanisms, steal passwords or data, or crack passwords;
  - Attempt to consume all of an available system resource intentionally;
  - Replicate themselves or attach themselves to other programs, in the manner commonly called worms or viruses;
  - Are designed to evade software licensing or copying restrictions;
  - Scan the network to identify security vulnerabilities.
- Users who believe that they have a legitimate reason to use or develop programs in the above categories must obtain permission from the Chief Information Officer or delegate, before developing or using such programs.
- The integrity of the CIB operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.

System testing and acceptance

- New applications, changes and/or fixes to existing applications for use on CIB production servers must be tested and approved/accepted by the responsible business owner and approved for production readiness by the relevant Chief Information Officer.
- Tests must be performed prior to any IT equipment or software applications entering the operational phase to ensure that security are in order and according to requirements

Changes to systems

- Change control procedures must be utilised for all changes to systems. All changes to programs must be authorised and tested before moving to the live environment.
- Emergency change requests may only be performed according to emergency change procedures.

Data Security

- All CIB confidential data must be backed up on a daily basis.
- All CIB data residing on individuals machines is the responsibility of the user.
- All CIB data that is taken off-site must be encrypted.
- Data users acknowledge that they will only use CIB data under the following terms and conditions:
  - That the data is used only for the purposes specified by the data owner;
  - That the user will comply with all security measures as stipulated by the owner;

- All data generated by and for the CIB business is the property of CIB and may not be copied, downloaded, or taken out of the company by any means;
- Not to disclose any of the data or information around access controls to the data unless specifically authorised to do so.

- Sensitive or confidential data/information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured.
- In the case of e-mails, with or without attachments, the Sender of the e-mail must ensure that the confidentiality and integrity of the data/information being sent is maintained.

Software Licensing

- Audits must be performed at least annually to compare software in use within CIB against the list of legal software.
- Any software to be installed on any device in CIB must be original and properly licensed from the proper source authorised to distribute the software.

Maintenance of IT equipment

- All computer workstations must be configured for security safety according to standard image configuration as determined by CIB IT department.
- No devices may be connected to any network or public circuit, unless performed by CIB IT or its delegates.

Backup and recovery

- Information system owners are responsible for defining adequate backup and system recovery requirements.
- IT Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.
- Unless otherwise stated and agreed, backup and system recovery will be performed according to the Backup Procedure and IT Disaster and Recovery Plan.
- Information and data stored on a laptop or portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

Media Handling

- Software and backup media must be stored (on or off-site) using fire protected storage cabinets. A register must be kept up to date with adequate check in/out controls.
- Backup media in transit must be protected at all times.
- The storage media used for the archiving of information must be appropriate to its expected life span.
- The format in which the data is stored must be carefully considered, especially where propriety formats are involved.

Business requirement for access control

- Access control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs.
- Access controls for highly sensitive information or high risk systems must be set in accordance with classification and value of the information assets being protected.
- High risk systems require more stringent access control safeguards due to the confidentiality of the information they process and/or the purpose of the system. The operating systems for such systems must be elevated to further enhance such systems.

User access management

- Access to all systems must be authorised by the owner/s of the system.

- Access to electronic files and documents must be controlled to ensure that only authorised personnel have access to sensitive information.
- Each user account must be owned, used and identified by a single person.

Secure access

- The site or areas chosen to house computer data centres and data storage must be suitably protected against theft, fire, flood, and other identified hazards. Secure areas must be safeguarded against unlawful and unauthorised physical intrusion. All server rooms, computer data centres, secure locations and data storage facilities must be locked at all times.

Physical security

- Physical access to secure areas must be suitably controlled.
- All CIB server rooms must be locked at all times. Only CIB IT Infrastructure team will have control access to the server room.
- Access to the server room will be restricted to the CIB IT Infrastructure team only. Other staff and contractors requiring access to the server room will notify the Chief Information Officer in advance so that the necessary supervision can be arranged.
- An intruder alarm incorporating the following features must be installed: remote monitoring, armed response and maintenance by an approved company.
- All CIB server rooms must contain adequate air conditioning systems to provide a stable operating environment to reduce the risk of system crashes due to component failure.
- No water, rain water or drainage pipes must run within or above the server rooms to reduce the risk of flooding.
- The floor within the server room must be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.
- UPS power must be provided to the server room to help protect the computer systems in the case of a mains power failure. Where possible, generator power should feed the UPS power.
- All UPS's, Fire protection system and Generators will be tested / checked periodically.
- In case of a disaster or emergency no access to the Server Room is allowed unless supervised.

Disposal of IT assets

- Only authorised personnel, who have ensured that the relevant security risks have been mitigated, may dispose of IT equipment owned by CIB.
- All applicable CIB licensed software, data and information, must be removed prior to disposal.

Report incidents

- An Information Security incident is any occurrence, which in itself does not necessarily compromise Information Security but could result in it being compromised. All Information pertaining to Security incidents must be reported promptly to the CIB IT department as well as any other relevant department head.
- Breaches of confidentiality arise from a breach of an employee's Terms and Conditions of Employment and / or from non-compliance with a Non-disclosure Agreement. Such breaches must be seen as an Information Security incident and treated accordingly.
- Virus incident response must be regularly reviewed and tested.

Response to incidents

- Suitably qualified and trained personnel must investigate Information Security incidents. The investigation into such incidents must identify its cause and appraise its potential damage to the system or data.
- Collection, recording and processing of evidence relating to suspected Information Security breaches must be authorised by the Chief Information Officer.
- CIB IT department must respond rapidly and calmly to all reports of Information Security incidents / breaches, liaising and coordinating with relevant departments, depending on the particular circumstance.
- Maintaining confidentiality about Information Security Incidents whilst they are being investigated is imperative for CIB's reputation. Only authorised persons may release information relating to such incidents.

Security investigations

- Security investigations may involve the unrestricted access (by an individual or team responsible for the investigation) to the CIB user directory information and contents, CIB access activities and computer resources by using technologies with unrestricted access.
- No organisation or individual may initiate or conduct security investigations without the consent of Chief Information Officer.
- Approval must be obtained from the Chief Information Officer to send data collected from the CIB IT Operations to the approved investigative agency prior to sending such information.
- Management must ensure that:
  - Information being disclosed is appropriate to the investigation;
  - CIB Legal department approves with regard to any applicable privacy laws;
  - Information not appropriate to the investigation is excluded;
  - Information is in a format usable by 3rd parties;
  - Media shall be labelled as confidential where applicable;
  - Where applicable, the receiving party of such information must be under a specific non-disclosure agreement to receive such information.

Independent review

Management will ensure that the implementation of IT security is reviewed by an independent party upon implementation and yearly thereafter.

Non-compliance

All users defined in the scope above will be required to confirm their acknowledgement and acceptance of this policy. Any users found to have violated these guidelines, may be subject to disciplinary action, up to and including termination of employment in terms of the company's disciplinary code.

Annexure M

PRIVACY POLICY

Introduction

The Protection of Personal Information Act No 4 of 2013 (POPIA) requires us to ensure that you are aware of how we collect, use and disclose personal information we obtain from you or your broker.

What information is being collected and processed?

Personal information as defined by the POPIA needed to provide insurance cover and settle claims.

Voluntary/Mandatory

You are required to provide the information voluntarily and you understand that the same is mandatory for purposes of entering into an insurance contract with the insurer.

Why is the information being processed?

This will enable you to enter into an insurance contract with the insurer and to ensure that your risk is correctly assessed [including obtaining your credit information at any stage from TransUnion Credit Bureau (Pty) Ltd, Experian Information Solutions Inc. or XDS (Pty) Ltd] in order to provide you with the best suited insurance cover. We use your personal information to do the following:

- To identify you.
- For underwriting purposes.
- Conducting credit reference searches or verification.
- To renew and manage your policy.
- To amend your policy.
- To assess and settle claims.
- To detect and prevent fraud.
- To comply with the relevant clause of South Africa including but not limited to POPIA.
- Conducting market or customer satisfaction research.
- For audit and record keeping purposes.
- In connection with legal proceedings.

What is the source?

From the potential policyholder (you) directly or from your appointed broker.

Cross border transfer

Where necessary, the information may be shared with reinsurers in countries who subscribe to similar data protection laws. Where the information is shared with reinsurers which do not subscribe to similar data protection laws, CIB will enter into an agreement with such entity in terms whereof such entity will be liable to the protection of the personal information.

How is the information being processed?

The information is uploaded onto our internal IT system where it is stored and used to assess your risk profile, issue you with a policy and process claims. We have taken adequate security measures to ensure the integrity and security of your personal data.

Where is the information being processed?

We process the information at our head office in Bedfordview or at any of our branches.

Will the information be given to anyone else?

Yes, but only where necessary. It will be given to the insurer, reinsurers, your broker, product suppliers, service providers, credit bureau and any regulatory organisation.

Access and right to amend

You have the right to access and amend his/her personal information at any reasonable time.

Your rights

You are entitled to object to the use of information. However, such objection may lead to CIB being unable to provide insurance cover. You have the right to:

- access the information at any reasonable time for purposes of rectification thereof.
- object to the processing of the information in which case CIB will be unbale to facilitate insurance cover in accordance with the provisions contained herein.
- lodge a complaint to the Information Regulator

Security measures in respect of personal information

The POPIA requires us to secure the integrity and confidentiality of your personal information in our possession or under our control to avoid unauthorised access and use of your personal information. We continuously review our security controls and processes to ensure that personal information is secure. If we need to transfer personal information elsewhere for processing or storage, we will ensure that any party to whom we pass on your personal information will treat your information with the same level of protection as required from us.

CIB's contact details (Responsible party):

Physical address

15E Riley Road, Riley Road Office Park, Bedfordview, Gauteng, 2008

Postal address

Private bag x1600, Bedfordview, 2008

Telephone: 011 455 5101

Information Officer: Douglas Donnelly

Deputy Information Officers: Douglas Donnellyand Shoaib Nathie

Email: popia@cib.co.za

Annexure N

Clean Desk Policy

Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information. This policy supports compliance with the POPI Act, Condition 7: Security safeguards.

Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site.

Scope

This policy applies to all CIB employees and contractors.

Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
4.2 Computer workstations must be locked when workspace is unoccupied.
4.3 Computer workstations must be shut completely down at the end of the work day.
4.4 Any confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
4.7 Laptops must be either locked with a locking cable or locked away in a drawer.
4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
4.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
4.10 Upon disposal confidential documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
4.11 Whiteboards containing confidential information should be erased.
4.12 Lock away portable computing devices such as laptops and tablets.

4.13 Treat mass storage devices such as CDROM, DVD or USB drives as a potential for risk of loss and secure them in a locked drawer.

4.14 All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that confidential documents are not left in printer trays for the wrong person to pick up.

Policy Compliance

5.1 Compliance Measurement

The CIB management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the CIB management team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.