PROTECTION OF PERSONAL INFORMATION POLICY

August 2021

Revised November 2023

ABCUS INVESTMENTS CC (Registration number 2003/077702/23) TRADING AS ABCUS WINDOWS & DOORS

(Vat registration no. 4610209183)

PO Box 37, Montana Park, 0159,

Pretoria

INDEX

PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 (POPIA)

PROMOTION OF ACCESS TO INFORMATION ACT, 2000 (PAIA)

PAGE

INDEX

PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 (POPIA)

PROMOTION OF ACCESS TO INFORMATION ACT, 2000 (PAIA)

PAGE

1. INTRODUCTION

1.1 This "Protection of Personal Information Policy" describes the way that Abcus Investments CC, trading as Abcus Windows & Doors, will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the **Protection of Personal Information Act, No. 4 of 2013 (PoPIA) and the Promotion of Access to Information Act, Act 2 of 2000 (PAIA)**, as these Acts are the key pieces of legislation covering security and confidentiality of personal information.

1.2 Abcus Windows & Doors is committed to protect its customer's and employee's ("Data Subject's") privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

1.3 The Policy sets out the manner in which Abcus Windows & Doors deals with our customers' and employees' Personal Information as well as it stipulates the purpose for which said information is used.

1.4 "Data Subjects" refer to the persons to whom personal information relates.

1.4.1 Within an employment context, this includes applicants and former job applicants (successful or unsuccessful), former or current employees, temporary employment employees, casual employees, employees on learnership and those on work experience placements.

1.4.2 Within a business context it includes for example legal entities, customers, organisations, individuals, corporations, partnerships, cooperatives, customer groups and/or suppliers.

1.4.3 The simplest and most obvious categorisation of Data Subjects for Abcus Windows & Doors' business purposes would be the context of different types of people, natural or juristic, that the company works with. These types of people are customers, suppliers and employees.

1.5 The personal information of all of these "Data Subjects" must be dealt with in accordance with PoPI Act, PAIA Act and Abcus Windows & Doors' Protection of Personal Information Policy.

1.6 This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within Abcus Windows & Doors and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their Personal information

2. BACKGROUND

2.1 The purpose of the PoPI & PAIA Acts are to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another person's and/or entity's personal information by holding the institution like, Abcus Windows & Doors, accountable should they abuse or compromise personal information in any way. The PoPI & PAIA Act legislation basically consider that personal information to be "precious goods" and therefore aims to bestow the person and/or entity, as the owner of the personal information ("Data Subject"), certain rights of protection and the ability to exercise control over it.

2.2 Abcus Windows & Doors needs to ensure that when and how an individual and/or entity (Data Subject) choose to share their information (requires their consent) the type and extent of the information the person and/or entity choose to share (must be collected for valid reasons) is:

- transparent and can be accounted for on how the data will be used (limited to the purpose);
- receive notification if/when the data is compromised providing the person and/or entity with access to their own information; and
- the person and/or entity has as the right to have their data removed and/or destroyed should they wish so.

2.3 Therefore Abcus Windows & Doors must implement adequate measures and controls to track access and to prevent unauthorised people, even within the company, from accessing personal information.

2.4 The information must be adequately stored and controls must be in place to safeguard the person's and/or entity's information to protect it from theft, or being compromised.

2.5 Furthermore the information must be captured correctly and once collected, kept safe and accurately to guarantee integrity.

2.6 Each person ("Data Subject") also has the obligation to take care and protect their own information. Individuals and/or entities also need to be careful when sharing personal information not to compromise themselves. Abcus Windows & Doors shall however ensure to safeguard individuals' and/or entities' personal information.

3. SCOPE OF THE POLICY

3.1 The Policy applies to all employees, members, directors, customers/clients, sub-contractors, suppliers' independent contractors, any third party the company may and/or will deal with, agents, and appointees.

3.2 The provisions of the Policy are applicable to both on and off-site processing of personal information.

4. POLICY STATEMENT

4.1 Abcus Windows & Doors collects and uses Personal Information of Data Subjects with whom it works in order to operate and carry out its business effectively. The company regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the company and those individuals and entities who we deal with. Abcus Windows & Doors therefore fully endorses and adheres to the principles of the Protection of Personal Information Act (PoPI Act) and the Promotion of Access to Information Act (PAIA Act).

5. PERSONAL INFORMATION AND SPECIAL PERSONAL INFORMATION

5.1 Personal Information

5.1.1.1 In terms of the PoPI Act, ''Personal Information'' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. Abcus Windows & Doors may make use of a formal Consent by Data Subject form (e.g., customers, suppliers, employees)" to collect and use Personal Information (Annexure A & B).

5.1.1.2 "A living natural person" implies that if the person has died their personal information no longer falls within the scope of the POPI Act.

5.1.1.3 "An existing juristic person" means a legal entity that has not ceased to exist. Thus, if the juristic person ceases to exist its personal information no longer falls within the scope of the POPI Act.

5.1.1.4 Personal Information is 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 (examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence) 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.

5.2 Special Personal Information

5.2.1 Section 26 of the PoPI Act creates a special category of personal information called “special personal information”. This relates to

- Religious or philosophical or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour; and
- Information concerning a child.

5.2.2 Abcus Windows & Doors may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons; and
- If processing of race or ethnic origin is in order to comply with affirmative action laws for example Employment Equity- and Skills Development reports

5.2.3 All Data Subjects have the right to refuse or withdraw their consent to the processing of their personal information and a Data Subject may object, at any time, to the processing of their personal information. If the Data Subject withdraws consent or objects to processing then Abcus Windows & Doors shall forthwith refrain from processing personal information.

5.3 Exceptions for Processing Special Personal Information

5.3.1 There are exceptions for gathering and processing personal information. The following table is applicable to Abcus Windows & Doors (there may be other exceptions in other circumstances and or in other entities):

EXCEPTION	EXPLANATION
Consent is given	Where a Data Subject (individual and/or entity) consents to the processing of their special personal information, a responsible party is permitted to process the special personal information.
Compliance with applicable legislation	In respect of race, ethnic origin, religious view, health or sex life can it be processed if it is necessary for the implementation of the provisions of law or for the reintegration of, or support for employees' benefits in connection with sickness or incapacity and/or legislation requirements.

5.3.2 Abcus Windows & Doors is guided by the eight conditions for lawful processing of personal information and only require a Data Subject to disclose information which is relevant and is necessary to achieve the purpose for which it is being collected.

6. THE EIGHT CONDITIONS FOR LAWFUL PROCESSING

6.1 The PoPI & PAIA Acts are implemented by abiding by eight processing conditions. Abcus Windows & Doors shall abide by these principles in all its possessing activities.

6.2 The eight information protection conditions are the following:

Condition 1: Accountability
Condition 2: Processing Limitation
Condition 3: Purpose Specification
Condition 4: Further Processing Limitation
Condition 5: Information Quality
Condition 6: Openness
Condition 7: Security Safeguards
Condition 8: Data Subject Participation

6.3 Abcus Windows & Doors will follow these eight conditions when processing personal information:

PRINCIPLE	EXPLANATION
1. Accountability	• Abcus Windows & Doors has appointed a party (Information- and Deputy Information Officer) who will be responsible for ensuring that the information protection principles within PoPIA & PAIA Acts and the controls that are in place to enforce them are complied with
2. Processing Limitation	• All personal information will only be processed in a fair and lawful manner that does not infringe the privacy of the Data Subject. • Personal information collected will be adequate, relevant and not excessive. • Collection of personal data will be collected directly from the Data Subject except as otherwise provide in the PoPI Act. That is if: ❖ the information is contained in or derived from a public record or has deliberately been made public by the Data Subject; ❖ the Data Subject or a competent person where the Data Subject is a child has consented to the collection of the information from another source; ❖ collection of the information from another source would not prejudice a legitimate interest of the Data Subject; ❖ collection of the information from another source is necessary for example the South African Revenue

PRINCIPLE	EXPLANATION
	Services Act, a court, national security and/or to maintain legitimate interest of the responsible party or third party; ❖ compliance would prejudice (impair) a lawful purpose of the collection; or ❖ compliance is not reasonably practicable in the circumstances of the particular case.
3. Purpose Specification	• Personal information will be collected for a specific purpose and the Data Subject from whom the personal information is collected will be made aware of the purpose for which the personal information was collected.
4. Further Processing Limitation	• Personal information will be collected for a specific purpose and the Data Subject from whom the personal information is collected will be made aware of the purpose for which the personal information was collected. • Further processing will be regarded as compatible with the purpose of collection if: ❖ Data Subject has consented to the further processing; ❖ Personal Information is contained in a public record; ❖ Personal Information has been deliberately made public by the Data Subject; ❖ Further processing is necessary to maintain, comply with or exercise any law or legal right; or ❖ Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party. • It will have a lawful purpose related to the function or activity of Abcus Windows & Door's business.
5. Information Quality	• Abcus Windows & Doors shall take reasonable steps to ensure that the personal information that has been collected is complete, accurate, not misleading and up to date. • Employees should as far as reasonably practically follow the following guidance when collecting personal information: ❖ Personal information should be dated when received; ❖ A record should be kept of where the personal information was obtained from; ❖ Change to information records should be dated; ❖ Irrelevant or unneeded personal information should be deleted or destroyed; and/or ❖ Personal information should be stored securely, either on a secure electronic database or in a secure physical filling system.

PRINCIPLE	EXPLANATION
6. Openness	• "Openness" is linked directly to Abcus Windows & Doors' duty to process information in a fair and transparent manner. • Abcus Windows & Doors shall take "reasonably practicable" steps to ensure that the Data Subject has been made aware that his or her personal information is going to be collected. • The Data Subject will be made aware of: ❖ What personal information is collected and the source of information; ❖ The purpose of collection and processing; ❖ Where the supply of personal information is voluntary or mandatory and the consequences of a failure to provide such information; ❖ Whether collection is in terms of any law requiring such collection; ❖ Whether the personal information shall be shared with a third party.
7. Security Safeguards	• Abcus Windows & Doors shall ensure the integrity and confidentiality of all personal information in its possession, by taking reasonable steps to: ❖ Identify reasonably foreseeable risks to information security; and ❖ Establish and maintain appropriate safeguards against such risks. • Written records: ❖ Personal information records should be kept in locked cabinets and/or offices; ❖ When in use personal information records should not be left unattended in areas where non-authorised people may access it; ❖ Abcus Windows & Doors shall implement a clean desk policy where all employees shall be required to clear their desks of all personal information when leaving their desks for any length of time and at the end of the day; ❖ Personal information which is no longer required must be disposed of by shredding. ❖ Any loss or theft of or unauthorised access to personal information must be immediately reported to the Information Officer.

PRINCIPLE	EXPLANATION
	• Electronic records: ❖ All electronic records must be saved in a secure database; ❖ As far as reasonably practicable no personal information should be saved on individual computers, laptops or hand-held devices; ❖ All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonably complexity and changed frequently; ❖ All employees shall be required to lock their computers or laptops when leaving their desks for any length of time and log off at the end of the day; ❖ All electronic personal information must be deleted from the computer, laptop and/or database. It must be ensuring that the information has been completely deleted and is not recoverable. • Any loss or theft of computers, laptops or any other devices which may contain personal information must be immediately reported to the Information Officer, who shall notify the relevant knowledgeable person, who shall take all the necessary steps to remotely delete the information, if possible.
8. Data Subject Participation	• Data Subjects are empowered to access and/or request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated. • All such requests must be submitted in writing to the Information Officer • Unless there are grounds for refusal, Abcus Windows & Doors shall disclose the requested personal information: ❖ On receipt of adequate proof of identity from the Data Subject, or requester; ❖ Within a reasonable time; ❖ On receipt of the prescribed fee, if any; ❖ In a reasonable format. • Abcus Windows & Doors shall not disclose any Personal information to any party unless the identity of the requester has been verified.

7. PROCESSING PERSONAL INFORMATION

7.1 Purpose of Processing

7.1.1 Section 9 of PoPI Act states that “Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.”

7.1.2 Abcus Windows & Doors uses Personal Information under its care in the following ways:

- Administering employee benefits;
- Administering of agreements;
- Complying with legal and regulatory requirements;
- Conducting auditing and monitoring of transactions and engagement;
- Conducting business analysis, such as analytics, projections and identifying areas for operational improvement;
- Conducting credit reference checks and assessments;
- Conducting market or customer satisfaction research;
- Conducting business research and development;
- Confirming, verifying and updating customer details;
- Creating and maintaining the Data Subject’s account;
- Day to day employee management;
- Fulfilling Abcus Windows & Door’s legal functions or obligations;
- Keeping of accounts and records;
- Marketing and sales;
- Providing products and/or information to customers;
- Recruiting and selecting of new employees;
- Termination of employment; and/or
- Updating our operational and technical functionality.

7.2 Categories of Data Subjects and their Personal Information

7.2.1 Abcus Windows & Doors may process records relating to employees, suppliers, shareholders, contractors, entities, service providers, independent contractors and customers.

7.2.2 The following table indicates some of the Data Subjects’ Personal Information Abcus Windows & Doors may process:

ENTITY TYPE	PERSONAL INFORMATION PROCESSED
Customers: Natural persons	Names; contact details; physical and postal addresses; ID number; tax related information; nationality; banking details, Copy of ID, Banking details.
Customers: Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information, VAT registration number, Type of business, registration number, Trade References, Financial- or management statements, ID Copies of all members / directors / owners, Copy of Registration certificate, Copy of company registration certificate
Contracted Service providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information, banking details.
Employees / Directors / members	Gender; pregnancy; marital status; colour, race; age; language; marital status, education information; financial information; employment history; Copy of ID; physical and postal address; contact details; opinions; criminal record; well-being, banking details, salary details, performance reviews, next of kin details, Copies of next of kin nominated, passport number, vehicle license, job title, disciplinary records, drug and alcohol test results, Third party review of new applicants (references)

7.3 Categories of Recipients for Processing the Personal Information

7.3.1 Abcus Windows & Doors may share the Personal Information with its service providers, agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services.

7.3.2 Abcus Windows & Doors may supply the Personal Information to any party to whom Abcus Windows & Doors may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Banking institutions;
- Government institutions in order to comply with legislative requirements e.g., SARS, Compensation Commissioner, Seta's;
- Financial services suppliers e.g., accounting firms;
- Sending of emails and other correspondence to customers;
- Conducting due diligence checks; and/or
- Administration of the Provident and Group Risk Schemes.

7.4 **Actual or Planned Transborder Flows of Personal Information**

7.4.1 Personal Information may be transmitted transborder to Abcus Windows & Doors' authorised dealers and its suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws.

7.4.2 Abcus Windows & Doors will endeavour to ensure that its dealers and suppliers will make all reasonable efforts to secure said data and Personal Information.

7.5 **Retention of Personal Information Records**

7.5.1 Abcus Windows & Doors may retain Personal Information records indefinitely, unless the Data Subject objects thereto.

7.5.2 If the Data Subject objects to indefinite retention of its Personal Information Abcus Windows & Doors shall retain the Personal Information records to the extent permitted or required by law.

7.6 **General Description of Information Security Measures**

7.6.1 Abcus Windows & Doors employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures may include:

- Firewalls;
- Virus protection software and update protocols;
- Logical and physical access control; and
- Secure setup of hardware and software making up the Information Technology infrastructure.

8. IMPLEMENTATION GUIDELINES

8.1 Dissemination of Information

8.1.1 This Policy has been put in place throughout Abcus Windows & Doors, information about the Policy, PoPI Act and PAIA Act will take place with all affected employees.

8.1.2 All new employees will be made aware at induction, or through training programmes, or through informational documents of their responsibilities under the terms of this Policy, PoPI Act and PAIA Act. Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all employees.

8.2. Employee Contracts

8.2.1 Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

8.2.2 Each employee currently employed within Abcus Windows & Doors will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Employees are obliged to sign “Employee Consent and Confidentiality Clause” (Annexure B). Failure to comply will result in the instigation of a disciplinary procedure.

9. DESTRUCTION OF DOCUMENTS

9.1. Documents may be destroyed after the termination of the retention period specified herein, or as determined by Abcus Windows & Doors from time to time.

9.2. Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by Abcus Windows & Doors pending such return.

9.3. The documents must made available for collection by an approved document disposal company or shredded by Abcus Windows & Doors.

9.4. Deletion of electronic records must be done in consultation with the Information Technology and/or knowledgeable person, to ensure that deleted information is incapable of being reconstructed and/or recovered.

10. STATUTORY RETENTION PERIODS

10.1 In accordance with the POPI and PAIA Acts, Abcus Windows & Doors hereby provides the following information:

LEGISLATION	DOCUMENT TYPE	PERIOD
Companies Act	• Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act • Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities • Copies of reports presented at the annual general meeting of the company • Copies of annual financial statements required by the Act • Copies of accounting records as required by the Act • Record of directors and past directors, after the director has retired from the company; • Minutes and resolutions of directors' meetings, audit committee and directors' committees.	7 Years
Companies Act	• Registration certificate • Memorandum of Incorporation and alterations and amendments • Rules • Securities register and uncertified securities register • Register of auditors	Indefinitely
Consumer Protection Act	• Full names, physical address, postal address and contact details • ID number and registration number; • Contact details of public officer in case of a juristic person • Service rendered • Intermediary fee • Cost to be recovered from the consumer • Frequency of accounting to the consumer • Amounts, sums, values, charges, fees, remuneration specified in monetary terms • Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided	3 Years

LEGISLATION	DOCUMENT TYPE	PERIOD
	• Record of advice furnished to the consumer reflecting the basis on which the advice was given • Written instruction sent by the intermediary to the consumer • Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions • Documents Section 45 and Regulation 31 for Auctions.	
Financial Intelligence Centre Act	• Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer • If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person • If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer • The manner in which the identity of the persons referred to above was established • The nature of that business relationship or transaction • In the case of a transaction, the amount involved and the parties to that transaction • All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction • The name of the person who obtained the identity of the person transacting on behalf of the accountable institution • Any document or copy of a document obtained by the accountable institution	5 Years

LEGISLATION	DOCUMENT TYPE	PERIOD
Compensation of Occupational Injuries and Diseases Act	• Section 81(1) and (2) of the Compensation for Occupational Injuries and Diseases Act requires a retention period of 4 years for the documents mentioned below: • 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

	• Section 20(2) documents with a required retention period of 3 years:
	  • Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation
	  • Records of incidents reported at work.
		3 Years

	• Asbestos Regulations, 2001, regulation 16(1) requires a retention period of minimum 40 years for the documents mentioned below:
	  • Records of assessment and air monitoring, and the asbestos inventory;
	  • Medical surveillance records
		40 Years

	• Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):
	  • Records of risk assessments and air monitoring;
	  • Medical surveillance records.
		3 Years

	• Lead Regulations, 2001, Regulation 10:
	  • Records of assessments and air monitoring;
	  • Medical surveillance records.
		3 Years

	• Noise - induced Hearing Loss Regulations, 2003, Regulation 11:
	  • All records of assessment and noise monitoring
	  • All medical surveillance records, including the baseline audiogram of every employee.
		3 Years

	• Hazardous Chemical Substance Regulations, 1995, Regulation 9 requires a retention period of 30 years for the documents mentioned below:
	  • Records of assessments and air monitoring;
	  • Medical surveillance records.	

LEGISLATION	DOCUMENT TYPE	PERIOD

Basic Conditions of Employment Act	• Section 29(4):
	  • Written particulars of an employee after termination of employment
	• Section 31:
	  • Employee's name and occupation
	  • Time worked by each employee
	  • Remuneration paid to each employee
	  • Date of birth of any employee under the age of 18 years
		3 Years

Employment Equity Act	• Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act • Section 21 report which is sent to the Director General	3 Years

Labour Relations Act	• Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:
	  • The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings
	  • Registered Trade Unions and registered employer's organizations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings
	  • Registered Trade Unions and employer's organizations must retain the ballot papers
	  • Records to be retained by the employer are the collective agreements and arbitration awards.
	• Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents mentioned below:
	  • Registered Trade Unions and registered employer's organizations must retain a list of its members
	  • An employer must retain prescribed details of any strike action involving its employees
		3 Years
		
		Indefinite

LEGISLATION	DOCUMENT TYPE	PERIOD
	• Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions • The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.	
Unemployment Insurance Act	• The Unemployment Insurance Act, applies to all employees and employers except: • Workers working less than 24 hours per month • Learners • Public servants; • Foreigners working on a contract basis; • Workers who get a monthly State (old age) pension; • Workers who only earn commission. • Section 56(2)(c) requires a retention period of 5 years, from the date of submission, for the documents mentioned below: • Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.	5 Years
Tax Administration Act	• Section 29 of the Tax Administration Act, states that records of documents must be retained to: • Enable a person to observe the requirements of the Act • Are specifically required under a Tax Act by the Commissioner by the public notice; • Will enable SARS to be satisfied that the person has observed these requirements. • Section 29(3)(a) requires a retention period of 5 years, from the date of submission for taxpayers that have submitted a return and an indefinite retention period, until the return is submitted, then a 5-year period applies for taxpayers who were meant to submit a return. • Section 29(3)(b) requires a retention period of 5 years from the end of the relevant tax period for taxpayers who were not required to submit a return, but had capital gains/losses or engaged in	5 Years 5 Years

LEGISLATION	DOCUMENT TYPE	PERIOD
	any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption. • Section 32(a) and (b) require a retention period of 5 years but records must be retained until the audit is concluded or the assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.	5 Years
Income Tax Act	• Schedule 4, paragraph 14(1)(a) -(d) of the Income Tax Act requires a retention period of 5 years from the date of submission for documents pertaining to each employee that the employer shall keep: • Amount of remuneration paid or due by him to the employee • The amount of employees' tax deducted or withheld from the remuneration paid or due • The income tax reference number of that employee • Any further prescribed information; • Employer Reconciliation return. • Schedule 6, paragraph 14(a)-(d) requires a retention period of 5 years from the date of submission or 5 years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to: • Amounts received by that registered micro business during a year of assessment • Dividends declared by that registered micro business during a year of assessment; • Each asset as at the end of a year of assessment with cost price of more than R 10 000 • Each liability as at the end of a year of assessment that exceeded R 10 000	5 Years 5 Years

LEGISLATION	DOCUMENT TYPE	PERIOD
Value Added Tax Act	• Section 15(9), 16(2) and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, 30 March requires a retention period of 5 years from the date of submission of the return for the documents mentioned below: • Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; • Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS • Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques • Documentary proof substantiating the zero rating of supplies • Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 Years

11. REQUEST TO PERSONAL INFORMATION

11.1 Data Subjects have the right to:

- Request what personal information Abcus Windows & Doors holds about them and why;
- Request access to their personal information; and/or
- Be informed how to keep personal information up to date.

11.2 Access to Information request can be made by email, addressed to the Information Officer. The Information Officer will provide the Data Subject with a **"Request for access to record"– Form 2: Regulation 7)** (Annexure C). Once the completed form has been received, the Information Officer will verify the identity of the Data Subject prior to handing over any personal information. All requests will be processed and considered against the organisation's policies and procedures. The Information Officer will process all requests within a reasonable time.

11.3 Abcus Windows & Doors may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which Abcus Windows & Doors may refuse access include:

- Protecting personal information that Abcus Windows & Doors holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that Abcus Windows & Doors holds about a third party or Abcus Windows & Doors (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of Abcus Windows & Doors;
- Disclosure of the record would put Abcus Windows & Doors at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme; and

- The record contains information about research being carried out or about to be carried out on behalf of a third party or by Abcus Windows & Doors.

11.4 If Abcus Windows & Doors has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

12 COMPLIANTS PROCEDURE

12.1 Data Subjects have the right to Appeal ("Internal Appeal Form, Form 4 – Regulation 9", Annexure E), in instances where any of their right under PoPI and/or PAIA Acts have been infringed upon, Abcus Windows & Doors takes complaints very seriously and will address all PoPI and PAIA Acts related complaints in accordance with the following procedure:

12.1.1 PoPI and PAIA Acts complaints must be submitted to Abcus Windows & Doors in writing. Where so required, the Information Officer will provide the Data Subject with a "Internal Appeal Form, Form 4 – Regulation 9" (Annexure E).

12.1.2 Where the complaint has been received by any person other that the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within in one (1) working day.

12.1.3 The Information Officer will provide the complainant with a written acknowledgement of the receipt of the complaint within five (5) working days.

12.1.4 The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in PoPI and PAIA Acts.

12.1.5 The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have wider impact on Abcus Windows & Door's Data Subjects.

12.1.6 Where the Information Officer has reason to believe that the personal information of Data Subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with Abcus Windows & Door's Deputy Information Officer, Risk Manager, Information Technology Manager and and Chief Executive Officer where after affected Data Subjects and the Information Regulator will be informed of this breach.

12.1.7 The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Abcus Windows & Door's CEO within seven (7) working days of receipt of the complaint. In all instances, Abcus Windows & Doors will

provide reasons for any decision taken and communicate any anticipated deviation from the specified timeliness.

12.1.8 The Information Officer's response to the Data Subject may comprise any of the following:

- A suggested remedy for the complaint;
- A dismissal of the complaint and the reasons as to way it was dismissed; and/or
- An apology (of applicable) and any disciplinary action that has been taken against any employees involved.

12.1.9 Where the Data Subject is not satisfied with the Information Officer's suggested remedies, the Data Subject has the right to complain to the Information Regulator.

12.1.10 The Information Officer will review the complaints process to access the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found defective. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to PoPI Act related complaints.

13. MANAGEMENT CONTROL AND ENFORCEMENT

13.1 Information Officer and Deputy Information Officers

13.1.1 In order to comply with legislation, the Information Officer for Abcus Windows & Doors will be the **Managing Director or a duly authorised person** of the Company according to the requirements as defined terms of section 55 and 56 of the Protection of Personal Information Act 2013 (PoPIA) and section 1 or 17 of the Promotion of Access to Information Act, Act 2 of 2000 (See Annexure F for "Guidance note on Information Officers and Deputy Information Officers").

13.1.2 The Information Officer will be duly registered with the Information Regulator as is required by the applicable legislation after its establishment and will report to the Chief Executive Officer of Abcus Windows & Doors as may be applicable.

13.1.3 Abcus Windows & Doors will also designate where necessary, an appropriate number of Deputy Information Officers as described under Section 56 of the Protection of Personal Information Act 2013, read together with the prescriptions of Section 17 of the Promotion of Access to Information Act 2000.

13.1.4 The Deputy Information Officer/s will also be duly registered with the Information Regulator after establishment as is required, reporting directly to the Information Officer of the Company and will in conjunction with the Information Officer and Chief Executive Officer any other designated individuals as needed.

14. ACCESS AND CORRECTION OF PERSONAL INFORMATION

14.1 Customers have the right to access the Personal Information Abcus Windows & Doors holds about them ("Request of access to record", Form 2: Regulation 7 - Annexure C). Customers also have the right to ask Abcus Windows & Doors to update, correct or delete their personal information on reasonable grounds. Once a customer objects to the processing of their personal information, Abcus Windows & Doors may no longer process said personal information. Abcus Windows & Doors will take all reasonable steps to confirm its customer's identity before providing details of their personal information or making changes to their personal information.

14.2 The details of Abcus Windows & Doors Information Officer and office are as follows:

Information Officer	:	Amelia Venter
Telephone Number	:	(012) 803 - 8791
E-Mail Address	:	amelia@abcus.co.za
Deputy Information Officer	:	Dawie Erasmus
Telephone Number	:	(012) 803 - 8791
E-Mail Address	:	risk@abcus.co.za
Office Details		
Telephone	:	(012) 803 - 8791
Postal	:	PO Box 37, Montana Park, Pretoria, 0159
Physical	:	301 Zasm Street, Waltloo, Pretoria, 0189

14.3. The Information Officer is responsible for:

- Conducting a preliminary assessment ("Privacy Breach of Information Assessment, Annexure G). This toll will help aid the investigation;
- The development, implementation and monitoring of this policy and compliance framework;
- Ensuring that this policy is supported by appropriate documentation;
- Ensuring that documentation is relevant and kept up to date;
- Ensuring this policy and subsequent updates are communicated to relevant managers, representatives, staff and associates, where applicable.

14.4 All employees, subsidiaries, Suppliers, Independent contractors, business units, departments and individuals directly associated with Abcus Windows & Doors are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information and/or Deputy Information Officer.

15. BREACH OF INFORMATION

15.1 Infringement of Information

15.1.1 A breach of Information security event can be defined as “The actual or potential loss of personal data and/or any information that could lead to identity fraud or have any other significant impacts on individuals on the company” (Abcus Windows & Doors).

15.1.2 The prescriptions applicable to this matter will apply to all Abcus Windows & Doors employees and to all third-party service providers under contract with Abcus Windows & Doors.

15.1.3 The following are common examples of events, which includes, but is not limited to:

- Loss or damage to paper-based files containing classified or personal identifiable information;
- Loss of computer equipment due to crime or an individual’s carelessness;
- Loss of unencrypted computer media e.g., CD, cell phone, data stick, laptop or another portable device;
- Corrupted data;
- Access to inappropriate websites;
- Theft;
- Fraud;
- A computer virus;
- Successful hacking attack;
- Accessing a system or computer using someone else’s authorisation code (password), either fraudulently or by accident;
- Forced entry gained to a secure room/building housing classified information;
- Finding classified or confidential company information outside the company’s premises;
- Finding company paper or electronic records about identifiable individuals in any location outside of the company premises (e.g., recycling documents);
- Discussing employees or any other Data Subject’s personal information with someone else in an open area where the conversation can be overheard by outsiders;
- Personal identifiable information sent by insecure means/lost in transit (e.g., pay slips, HR records, financial statements, copies of ID documents, etc.);
- Unauthorised copying of, or removal of personal identifiable information;
- A fax, e-mail, any electronic message or paper document with personal identifiable information sent to the incorrect recipient;
- Unsecured handling of information storage systems/equipment during a period of disaster or serious damage to the company’s premises due to e.g., fire, flooding, earthquake, sabotage, etc.;

- Evidence of unauthorised cameras, monitoring devices, or listening equipment in offices;
- Suspicious unaccompanied persons wandering around on the company's premises;
- Allowing uncleared and/or un-identified third party or other contractor personnel to work on information security systems of the company;
- Evidence of unattended and unsecured information processing workstations not securely logged-off during the absence of the employee;
- Evidence of weak or no appropriate password management/log-on procedures; and
- Any violation of related security protocols that can possibly lead to the loss of classified information.

15.2 Reporting procedure

15.2.1 If there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the Company is obliged under Section 22, subsection 1 of the Protection of Personal Information Act to notify the Regulator and also (subject to subsection 3) the Data Subject of the event/incident:

1. *Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the responsible party must notify—*
   a) the Regulator; and
   b) subject to subsection (3), the Data Subject, unless the identity of such Data Subject cannot be established.

2. *The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.*

3. *The responsible party may only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.*

4. *The notification to a Data Subject referred to in subsection (1) must be in writing and communicated to the Data Subject in at least one of the following ways:*
   1. Mailed to the Data Subject's last known physical or postal address;
   2. sent by e-mail to the Data Subject's last known e-mail address;
   3. placed in a prominent position on the website of the responsible party;
   4. published in the news media; or
   5. as may be directed by the Regulator.

5. *The notification referred to in subsection (1) must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including—*
    1. *a description of the possible consequences of the security compromise;*
    2. *a description of the measures that the responsible party intends to take or has taken to address the security compromise;*
    3. *a recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and*
    4. *if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.*

6. *The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a Data Subject who may be affected by the compromise.*

15.2.3 Under this policy all Abcus Windows & Doors employees and third-party contractors to the Company are obligated to report any breach, or suspected breach of information security immediately to the Information Officer, or in his/her absence, to the Deputy Information Officer or to the Chief Executive Officer via a prescribed process.

15.2.4 The prescribed process for reporting any breach of information security event related to any personal information owned by, or under control Abcus Windows & Doors, will be that any person that has any knowledge or evidence of such an occurrence will be obliged to make a written report regarding the incident immediately after acquiring the knowledge or evidence of the incident to the Information Officer, or in his/her absence, to the Deputy Information Officer or to the Chief Executive Officer. The Information Officer will make an assessment on the breach assessment (“Privacy Breach Assessment Form”, Annexure G).

15.2.5 An Investigation to the breach A compulsory “Breach of Information Report” (Annexure H) must be fully completed by the person witnessing or discovering the incident immediately after the initial report and submitted to the Information Officer, or in his/her absence, to the Deputy Information Officer or to the Chief Executive Officer.

15.2.6 A “Breach of Information Investigation Report” (Annexure H) will assist the Chief Executive Officer to ensure procedures are reviewed and updated to reflect the lessons learned from the investigation.

15.2.7 Only the Chief Executive Officer will be mandated to make a factual of the incident in order to take whatever remedial steps necessary to contain the situation and also for the regulatory reporting of the incident to the Information Regulator, Data Subject and data owner where it is deemed to be appropriate and applicable.

15.2.8 No other employee or any third-party contractor of the Company will have any mandate to decide on the merits, or applicability of any reports in this category, unless specifically authorised to this effect in writing by the Chief Executive Officer.

15.2.9 Any violation of this prescription will be addressed via the Disciplinary Code, or the Third-Party Management prescriptions of the Company as is applicable.

15.3 Accountability

15.3.1 Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or non-compliance to the Company's policy prescriptions, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of the Company.

15.3.2 The contractual agreements of external third-party contractors to the Company will be subject to immediate suspension or termination in the sole discretion of the Chief Executive Officer of Abcus Windows & Doors, pending investigation and recommendations of the Information Officer and/or Deputy Information Officer and/or Chief Executive Officer and/or knowledgably employees of Abcus Windows & Doors. In the event of a monetary loss to Abcus Windows & Doors as a direct result of the occurrence of the breach in Information Security, the responsible party, or parties in both instances may be held fully liable for the loss and any costs for recovery thereof in the sole discretion of the Chief Executive Officer of Abcus Windows & Doors.

15.4. **Enforcement**

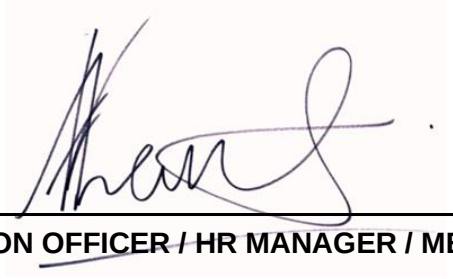
15.4.1 The severity of any disciplinary or other enforcement action taken by Abcus Windows & Doors will vary based on factors considered relevant by the Chief Executive Officer, including but not limited to:

- The sensitivity of the personal data disclosed or used in violation of this policy;
- The number of parties impacted by the violation of this policy;
- The duration of the improper disclosure or unauthorised use;
- Prior improper disclosure or use of personal information by any applicable accountable party; and/or
- Whether the violation or neglect was inadvertent or the result of inadequate training, or supervision.

16 AMENDMENTS TO THIS POLICY

16.2 Amendments to this Policy will take place on an ad hoc basis or as needed. Customers are advised to check our website periodically to inform themselves of any changes. Where material changes take place customers will be notified directly.

17 APPROVAL OF POLICY



INFORMATION OFFICER / HR MANAGER / MEMBER

Annexure: A

CONSENT BY DATA SUBJECT (CUSTOMERS / SUPPLIERS)

Abcus Windows & Doors understands that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a leaful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if your think that we have outdated information, please request us to update or correct it.

Our Information Officer can be contacted at:
Abcus Windows & Doors
Tel: - 012 – 803 8791
Email address: amelia@abcus.co.za or risk@abcus.co.za

Purpose for Processing your information:
We collect, hold, use and disclose your personal information mainly to provide you with access to the products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Providing you with advice on products and products that suits your needs as requested;
- To verify your identity and to conduct credit reference searches;
- To issue, administer and manage your credit / account with us;
- To notify you of new products, developments, price increases that may be of interest to you;
- To confirm, verify and update your details; and
- To comply with any legal and regulatory requirements.

Some of your information that we hold may include your first and last name, email address, an identity number, home address, a postal address or other physical address, other contact information, your title, birth date, gender, occupation, income, expenditure, your banking details.

Consent to Disclose and share your information
We may need to share your information to provide advice, analyses or services that your requested.

Where we share your information, we will take all precautions that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers manage by a third-party service provider, which may be locates outside South Africa.

I hereby authorise and consent to Abcus Windows & Doors to keep and share my information as necessary to provide the products and/or services as requested by me.

Name & Surname: _____

Signature: _____

Date: _____

Annexure: B

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

"PERSONAL Information" (PI) means information relating to an identifiable, living, natural or a juristic 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.

- "PoPIA" shall mean the Protection of Personal Information Act, Act 4 of 2013 and the "PAIA" shall mean Promotion of Access to Information Act, Act2 of 2000 as amended from time to time.

- The employer undertakes to process the PI of the employee only in accordance with the condition of lawful processing as set out in terms of PoPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions and an employer and within the framework of the employment relationship and as required by South African law.

- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions of the employer. The employee therefore irrevocably and unconditionally agrees:

    - That he/she is notified or the purpose and reason for the collection and processing of his/her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
    - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.

- Without derogating from the generality OF THE AFORESAID, the employee consents to the employer's collection and processing of PI pursuant to any of the employee's internet, email and other relevant policies insofar as PI of the employee is contained in relevant electronic communications.
- To make available to the employer all necessary PI required for the purpose of securing and further facilitating the employee's employment with the employer.
- To absolve the employer from any liability in terms of PoPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
- To disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI
- The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have to pursue a legitimate interest of the employer to perform its business on a day-to-day basis.
- The employee authorises the employer to transfer his/her PI outside the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

- The employer acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain customers, suppliers and other employees. The employee will treat all PI as a confidential business asset and agrees to respect the privacy of customers, suppliers and other employees.

- To the extent that he/she is exposed to or insofar as PI or other or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligation in relation to the PI of third parties or employees.

- Employees may not directly or indirectly, utilise, disclose or make public in any manner to any third party, either within the organisation or externally, any PI, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf the employer.

Name & Surname: _____

Signature: _____

Date: _____

Annexure: C

REQUEST FOR ACCESS TO RECORD

(Form 2 - Regulation 7)

Note:

1. Proof of identity must be attached by the requester
2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.

TO: The information officer
Abcus Windows & Doors
PO Box 37
Montana Park
Pretoria 0159
(Address)

E-mail address: amelia@abcus.co.za / risk@abcus.co.za

Mark with an "X"

Request is made in my own name ☐ Request is made on behalf of another person. ☐

PERSONAL INFORMATION	
Full names:	
Identity number:	
Capacity in which request is made (*when made on behalf of another person*):	
Postal Address:	
Street Address:	
E-mail Address	
Contact numbers: Tel. (B): Cellular: Facsimile	
Full names of person on whose behalf request is made *(if applicable*):	

Identity number:	
Postal Address:	
Street Address:	
E-mail Address:	
Contact numbers: Tel. (B): Cellular: Facsimile	
PARTICULARS OF RECORD REQUESTED Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)	
Description of record or relevant part of the record:	
Reference number, if available:	
Any further particulars of record:	

TYPE OF RECORD *(Mark the applicable box with an "X")*	
Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, cor generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	
FORM OF ACCESS *(Mark the applicable box with an "X")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription or virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive (*including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	
MANNER OF ACCESS *(Mark the applicable box with an "X")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (*including transcriptions)*	
E-mail of information *(including soundtracks if possible*)	
Cloud share/file transfer	
Preferred language: *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected:	
Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a) A request fee must be paid before the request will be considered. b) You will be notified of the amount of the access fee to be paid. c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record. d) If you qualify for exemption of the payment of any fee, please state the reason for exemption	
Reason:	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any.

Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication (*Please specify*)

Signed at _____ this _____ day of

_____ 20 _____

_____

Signature of requester / person on whose behalf request is made

……

FOR OFFICIAL USE

Reference number:	
Request received by: *(state rank, name and surname of information officer)*	
Date received:	
Access fees:	
Deposit (if any):	

_____

Signature of information officer

Annexure D

OUTCOME OF REQUEST AND FEES PAYABLE

(Form 3 - Regulation 8)

Note:

1. If your request is granted the—
   (a) amount of the deposit, (if any), is payable before your request is processed; and
   (b) requested record/portion of the record will only be released once proof of full payment is received.
2. Please use the reference number hereunder in all future correspondence.

Reference number: _____

TO: _____

_____

_____

_____

Your request dated _____, refers.

1. Your requested:

Personal inspection of information at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form) is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees as agreed upon in in Annexure C.	

OR

2. You requested:

Printed copies of the information (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)	
Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)	
Transcription of soundtrack (written or printed document)	
Copy of information on flash drive (including virtual images and soundtracks)	
Copy of information on compact disc drive (including virtual images and soundtracks)	
Copy of record saved on cloud storage server	

3. To be submitted:

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (including transcriptions)	
E-mail of information (including soundtracks if possible)	
Cloud share/file transfer	
Preferred language: (Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)	

Kindly note that your request has been:

☐ Approved

☐ Denied, for the following reasons:

4. Fees payable with regard to your request:

Item	Cost per A4-size page or part thereof/item	Number of pages/items	Total
Photocopy			
Printed copy			
For a copy in a computer-readable form on: i. Flash Drive • To be provided by the requestor ii. Compact Disk • If provided by the requestor • If provided to the requestor	 R40.00 R40.00 R60.00		
For a transcription of visual images A4-siz page	Service to be outsourced. Will depend on the quotation of the service provider		
Copy of visual images			
Transcription of an audio record, per A4-size	R24.00		
Copy of an audio record iii. Flash drive • To be provided by the requestor iv. Compact disk • If provided by the requestor • If provided to the requestor	 R40.00 R40.00 R24.00		
Postage, e-mail or any other electronic transfer	Actual costs		
To search for and prepare the record for disclosure, for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation.	Not to exceed a total cost of R 200.00 per hour		
TOTAL:			

5. Deposit payable (if search exceeds six hours):

☐ Yes

☐ No

Hours of search		Amount of deposit (calculated on one third of total amount per request)	

The amount must be paid into the following Bank account:
Name of Bank: _____
Name of account holder: _____
Type of account: _____
Account number: _____
Branch Code: _____
Reference No.: _____
Submit proof of payment to: _____

Signed at _____ this _____day of 20____

_____
Information officer

Annexure E

INTERNAL APPEAL FORM

(Form 4 - Regulation 9)

Reference Number: _____

PARTICULARS OF PUBLIC BODY				
Name of Public Body				
Name & Surname of Information Officer				
PARTICULARS OF COMPLAINANT WHO LODGES THE INTERNAL APPEAL				
Full Names				
Identity Number				
Postal Adress				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
E-Mail Address				
Is the internal appeal lodges on behalf of another person?	Yes		No	
If answer is "yes", capacity in which an internal appeal on behalf of another person is lodged: (Proof of the capacity in which appeal is lodged, if applicable, must be attached.)				
PARTICULARS of person on whose behalf the internal appeal is lodged (If lodged by a third party)				
Full Names				
Identity Number				
Postal Adress				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
E-Mail Address				

DECISION AGAINST WHICH THE INTERNAL APPEAL IS LODGED (mark the appropriate box with an "X")	
Refusal of request for access	
Decision regarding fees prescribed in terms of section 22 of the Act	
Decision regarding the extension of the period within which the request must be dealt with in terms of section 26(1) of the Act	
Decision in terms of section 29(3) of the Act to refuse access in the form requested by the requester	
Decision to grant request for access	

GROUNDS FOR APPEAL (If the provided space is inadequate, please continue on a separate page and attach it to this form. all the additional pages must be signed)	
State the grounds on which the internal appeal is based:	
State any other information that may be relevant in considering the appeal:	

You will be notified in writing of the decision on your internal appeal. Please indicate your preferred manner of notification:

Postal address	Facsimile	Electronic communication (Please specify)

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Appellant/Third party

FOR OFFICIAL USE

OFFICIAL RECORD OF INTERNAL APPEAL

Appeal received by: *(state rank, name and surname of Information Officer)*				
Date received:				
Appeal accompanied by the reasons for the information officer's decision and, where applicable, the particulars of any third party to whom or which the record relates, submitted by the information officer:		Yes		
		No		
OUTCOME OF APPEAL				
Refusal of request for access. Confirmed?	Yes		New decision (if not confirmed)	
	No			
Fees (Sec 22). Confirmed?	Yes		New decision (if not confirmed)	
	No			
Extension (Sec 26(1)). Confirmed?	Yes		New decision (if not confirmed)	
	No			
Access (Sec 29(3)). Confirmed?	Yes		New decision (if not confirmed)	
	No			
Request for access granted. Confirmed?	Yes		New decision (if not confirmed)	
	No			

Signed at _____ this _____ day of _____ 20 _____

_____

Relevant Authority

Annexure F

GUIDANCE NOTE ON INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS

The following documents are available on the Information Regulator's web page:

1. Information Officer's registration form

2. Designation and delegation of authority to the Deputy Information Officer

3. Authorisation of Information Officer

(InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf (justice.gov.za)

Annexure: G

PRIVACY BREACH OF INFORMATION ASSESSMENT

1. WAS PRIVATE INFORMATION INVOLVED?

Yes	
No	

2. DESCRIPTION OF BREACH

2.1 What data elements have been breached? E.g., identity numbers, contact details, financial information that could be used for identity theft ?

_____
_____
_____
_____
_____

2.2 What possible use is there for the Private Information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

_____
_____
_____
_____
_____

2.3 What was the date the breach was discovered? _____

2.4 What is believed to be the date that the breach occurred? _____

3 CAUSE AND EXTENT OF THE BREACH

3.1 What is the cause of the breach?

_____
_____
_____
_____
_____

3.2 Is there a risk of ongoing of further exposure of the information?

Yes	
No	

3.3 What was the extent of the unauthorised collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including mass media, online?

_____
_____
_____
_____
_____

3.4 What steps have already been taken to minimise the harm?

_____
_____
_____
_____
_____

4 INDIVIDUAL AFFECTED BY THE BREACH

4.1 How many individuals are affected by the breach? _____

4.2 Who was affected by the breach:

- ☐ Employees
- ☐ Customers
- ☐ Independent Suppliers
- ☐ Service Providers
- ☐ Other individuals /organisations: _____

5 FORESEEABLE HARM FROM THE BREACH

5.2 Is there any relationship between the unauthorised recipients and the data subject?

Yes	
No	

5.3 What harm to the individuals will result from the breach? Harm that may occur includes:

- ☐ Security risk (e.g. physical safety)
- ☐ Identity fraud of theft
- ☐ Loss of business or employment opportunities
- ☐ Hurt, humiliation, damage to reputation or relationships
- ☐ Other (please specify:

_____

_____

5.3 What harm could result to Abcus Windows & Doors as a result of the breach:

- ☐ Loss of trust in Abcus Windows & Doors
- ☐ Loss of assets
- ☐ Financial exposure
- ☐ Other (please specify:

_____

_____

6 OTHER COMMENTS

_____

_____

_____

_____

_____

_____ _____

Assessor's signature **Date**

Annexure H

BREACH OF INFORMATION REPORT

Directions:

- The reporting employee or witness needs to complete Section 1 and Section 2.
- If needed the employee or witness can consult with the relevant inhouse subject matter expert/s to complete section 2.
- All persons who contribute information to the report should be recorded in the "Report Augmented by" filed.
- When completed, the form should be submitted to the Information Officer with a copy to be retained by the reporting employee or witness and, if applicable, to be provided to the employee's Supervisor.
- Please print clearly.

SECTION 1: INCIDENT REPORTER	
Name & Surname	
Job Title	
Department	
Email Address	
Contact Number	
Report Submitted to – indicate name & surname	
SECTION 2: INCIDENT DETAILS	
Date and time of discovery of incident	
Estimated date and time incident started	

Description of incident (be specific, add additional pages to report if needed as well as evidence documents)	
Location of incident	
Current status of incident	
Source of incident	
Employees, Contractors or Others with knowledge of the incident (List all known potential witnesses)	
Mitigating factors	
Estimated impact of incident	
Response actions performed	
Other organisations contacted	
Report Augmented by	
Any additional Comments	

I understand that by submitting this Incident Report in good faith, I cannot be subject to retaliation. I attest that the information contained in this Incident Report is true and accurate to the best of my knowledge. If I obtain any additional information regarding this incident, I agree to provide said supplementary information to the person specified above in “Report to” and/or designated incident handler. I agree to cooperate fully with all investigations of this incident until the incident is closed.

Incident Reporter’s signature **Date**

Annexure: I

BREACH OF INFORMATION INVESTIGATION REPORT

Directions:

- Upon receipt of a "**Breach of Information Report"**, an investigation into the incident shall be initiated.
- The "**Breach of Information Investigation Report"**, should be completed as thoroughly as possible.
- Since Investigations vary, some sections may not be applicable to every investigation.

SECTION 1: INCIDENT INVESTIGATOR	
Date report received	
Name & Surname	
Job Title	
Email address	
Contact Number	

SECTION 2: INCIDENT UPDATE	
Summary of incident	

SECTION 3: INVESTIGATORS				
Name & Surname	Job Title	Organisation	Contact Number	Email address

SECTION 4: LOF OF ACTIONS TAKEN			
Date	Investigator	Action	Result

SECTION 5: EVIDENCE FOUND		
Date	Investigator	Evidence

SECTION 6: PARTIES INVOLVED IN INCIDENT				
Name & Surname	Job Title	Organisation	Contact Number	Email address

SECTION 7: INCIDENT INVESIGATORs' COMMENTENTS		
Date	Incident Investigator	Comments

SECTION 8:FINDINGS	
Malicious Conduct	☐ Yes ☐ No
Unauthorised Access	☐ Yes ☐ No
Inappropriate usages	☐ Yes ☐ No
Denial of service required	☐ Yes ☐ No
Other (specify)	
Cause of incident	
Cost of incident	
Business impact of incident	
Number of data subjects' PI are compromised	

SECTION 9: RECOMMENDED CORRECTIVE ACTION		
Recommended by	Date	Recommended corrective action

SECTION 10: ACTIONS TAKEN		
Recommended by	Date	Actions Taken

SECTION 11: NOTIFICATIONS MADE			
Organisation / Data Subject	Manner of contact	Date of notification	Summary of information provided

I attest that the information contained in this Investigation Report is true and accurate to the best of my knowledge and the knowledge of all contributors. I further attest that all parties who participated in the investigation, all findings of the investigation and all recommended corrective actions as well as all actions taken by any parties to this investigation are clearly documented. This Investigation Report has been provided to the Information Officer and Chief Executive Officer for review in both its final form and, as appropriate, throughout the term of the Investigation. Effective date indicated below; this Incident Investigation is considered closed.

_____ _____

Incident Investigator's Signature **Date**