POPIA POLICY

1. OBJECTIVE

1.1 Basson Blackburn Inc. & Blackburn Inc. are committed to collecting, storing and processing the Personal Information of our clients in a manner compliant with the Protection of Personal Information Act 4 of 2013 ("POPIA") and the Promotion of Access to Information Act 2 of 2000 ("PAIA").

1.2 Insofar as it is required in terms of POPIA, we will always obtain the written consent of our clients before processing your Personal Information in any way.

2. DEFINITIONS

2.1	"Personal Information":	"Information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person."
2.2	"Data Subject:"	"The person to whom Personal Information relates."
2.3	"Responsible Party:"	For purposes of this Notice, the Responsible Party is Basson Blackburn Inc. / Blackburn Inc.
2.4	"Consent:"	"Voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information."
2.5	"Processing:"	"Any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information."
2.6	"Record:"	"Any recorded information, regardless of form or medium, in the possession or under the control of a responsible party, whether or not it was created by a responsible party and regardless of when it came into existence."

2.7	"Regulator:"	"Information Regulator established in terms of Section 39."
2.8	"Special Personal Information:"	Personal Information of a data subject relating to their religious or philosophical beliefs; race of ethnic origin; trade union membership; political persuasion; health or sex life; biometric information and criminal behavior (to an extent).

3. GENERAL

3.1 Basson Blackburn Inc. / Blackburn Inc. and its employees undertake to treat all client information as strictly confidential.

3.2 No Personal Information regarding a client, or the content of any legal process, may at any time or by any means be divulged to an outsider by an employee.

3.3 No employee may request, gather or store any Personal Information from or regarding a client, unless this is done for business purposes and takes place with the full knowledge and consent of the client concerned. The information collected and processed is only used for the specified purpose for which it was intended, as set out at the time of procurement.

3.4 We undertake to provide access, upon request, to our clients and employees, to their own Record(s), in terms of the provisions of POPIA, and where sufficient proof of identity has been shown upon such request.

3.5 Where a client wishes to correct/update their Record(s), we request proof of the corrected/updated information before rectifying our documents to reflect the change. Proper record is also kept of the client's request to amend the details of their Record held by us, including the date of the request for the change as well as the change itself.

3.6 Where necessary, relevant and in the interest of properly carrying out our instructions and / or mandate, third parties are notified of changes to the details of a client.

3.7 There is no fee charged in relation to the request of a data subject for confirmation of whether we hold your Personal Information.

3.8 Where a data subject requests a Record or description of the Personal Information we hold, as well as that information to which third parties have access, we will attend to such a request "within a reasonable time; at a prescribed fee (if any); in a reasonable manner and format; and in a form that is generally understandable."

4. INFORMATION OFFICER

4.1 The details of our Information Officer and Deputy Information Officer are as follows:

4.1.1	Information Officer:	Deon Blackburn deonb@bassonblackburn.com 021 871 1401
4.1.2	Deputy Information Officer:	Caryn Fredericks caryn@bassonblackburn.com 021 871 1401

4.2 For any queries, requests or complaints related to the processing of Personal Information, please contact our Information Officer or Deputy Information Officer.

5. INCIDENT MANAGEMENT PROCESS

5.1 The processing of data, particularly by electronic means, is always accompanied by a certain element of risk. Although we do everything in our power to safeguard the integrity of the Personal Information entrusted to us, security breaches are still a possibility.

5.2 Where we have become aware of a data security breach / have reasonable grounds to believe that there has been a data security breach, this will be reported to the Information Regulator, as well as the data subject concerned, as soon as reasonably possible after becoming aware of the compromise / possible compromise, and we

will provide enough information to allow the data subject to act against any potential consequences.

6. RESEARCH REGARDING EMPLOYMENT APPLICATIONS

6.1 All applicants / prospective employees of Basson Blackburn Inc. / Blackburn Inc. are required to furnish certain details, within the ambit of the definition of "Personal Information," necessary for the consideration of their employment applications, including but not limited to, details of previous employment / work experience, identity numbers and contact details, for the purposes of background and reference checks.

6.2 Applicants / prospective employees confirm that the details of any and all references provided to us are so furnished with the express consent of the named person.

7. EMPLOYEE COGNISANCE OF POLICY

7.1 Employees of Basson Blackburn Inc. and Blackburn Inc., as part of their conditions of employment, attend a training workshop centred on dealing with the Personal Information of our clients in line with the provisions of POPIA. As and when the provisions and regulations are amended and/or supplemented, employees will be required to attend further workshops/training sessions, thereby ensuring that all employees remain up to date with the provisions of POPIA.

7.2 Each employee, therefore, is aware of the requirements for lawful processing of Personal Information and has undertaken to treat all client information as strictly confidential, both during and after their employment period.

7.3 Our Information Officer is responsible for updating and informing the employees of any relevant new regulations pertaining to POPIA and ensuring that they carry out their duties in line therewith.

8. DOCUMENTS CONTAINING PERSONAL INFORMATION

8.1 COMPUTERS

8.1.1 Only authorised employees (attorneys and support staff) have passwords and access to the firm's computers, main frame and printers.

8.1.2 By virtue of our internal privacy policy, these passwords are not shared with other computer users / divulged to any other person, except the authorised head of division.

8.1.3 Passwords are further changed regularly, with the view to improve/increase security.

8.1.4 Passwords and all other forms of access to the firm's main frame and information contained therein are immediately removed by the firm's IT agents upon an employee's termination of service.

8.2 PRINTERS

8.2.1 Documents that are printed in hard copy are immediately removed from the printers and filed in the appropriate file.

8.3 REMOVAL OF DOCUMENTS FROM OFFICE

8.3.1 In terms of our internal privacy policy, no files and/or documents containing the Personal Information of any client or employee may leave the premises without the prior approval of the head of department.

8.3.2 Such approval is only granted where the documents are removed exclusively for work purposes and the head of department is satisfied that the file/document will not fall into the hands of unauthorised persons.

8.3.3 Clauses 8.3.1 and 8.3.2 above also apply to electronic documents and correspondence. No document / information is removed from the office by means of a transportable hard drive or other storage device (e.g. USB stick) without the prior authorisation of the head of department.

8.3.4 Any document that leaves the office building is placed in a sealed envelope with the complete details of the addressee, as well as a return address in the case of non-delivery. These documents are taken to the

post office by hand, or by hand to the address of the addressee by an authorised employee of the firm.

8.3.5 Where the documents are transported by car, the documents are kept in the boot, which is locked.

8.3.6 Where documents are sent by courier, the services of a reliable/reputable courier company are utilised, and the documents are handed to the courier service in a sealed envelope.

8.3.7 Any document containing Personal Information of a client / employee is only handed to a person who is not in service of the firm where such a person has received a direct instruction to handle the document (e.g. correspondent / sheriff / clerk of the court) or to the person whose information is contained in the document.

8.3.8 Where a client / employee requests that the document be handed to a third party not employed by the firm (e.g. a proxy / messenger), a note this effect is made on the relevant file.

8.4 REMOTE COMPUTERS

8.4.1 Where employees are, for any reason, required to work from home/a location that is not 109 Main Road, Paarl, remote access is granted to such employees (attorneys and support staff), with the requisite security safeguards (passwords, anti-virus, firewall, etc.) in place to ensure that no unauthorised person gains access to the firm's main frame.

8.4.2 Employees are required to obtain prior authorisation from their head of department before removing his/her computer, or any component thereof, from the building.

9. RESTRICTION OF ACCESS TO OFFICES

9.1 All documents containing Personal Information, including all documents created and stored in electronic format, are kept within the premises known as 109 Main Road, Paarl.

9.2 All existing deeds files are kept in the firm's locked safe, and all other files are kept in the respective division's filing cabinets.

9.3 Documents in closed files are kept in the archives / storeroom, which is kept locked. The key is kept in a safe place and is only handed to authorised persons.

9.4 When closed files are destroyed after expiry of the prescribed period, the Information Officer ensure that the documents are properly destroyed, i.e. shredded.

10. ACCESS TO MAIN BUILDING

10.1 Both the front door and the security gate are locked at all times. The receptionist only grants access to authorised persons.

10.2 Documents containing Personal Information are not kept in the foyer, unless inside a sealed envelope.

10.3 Non-employees of/visitors to the firm are not permitted to leave the foyer area of the office to enter the rest of the building, unless accompanied by an employee of the firm, to ensure that the visitor does not gain access to any documents and/or information which does not apply to him/her.

10.4 Outside office hours, the building is kept locked at all times and the alarm activated by the last employee to leave the premises.

11. DESTRUCTION OF DOCUMENTS

11.1 Any paper on which Personal Information is printed, which is disposed of during the course of the work day but is not kept in the client file in the usual manner and eventually destroyed, is placed is separate containers from other waste materials.

11.2 The filing clerk in each department collects such papers daily to ensure that it is shredded before it may be removed, along with the rest of the day's waste, and destroyed.

12. RISK ANALYSIS

12.1 The Information Officer attends, on an annual basis, to an update on the firm's risk analysis report and data security safeguards, including the relevant measures pertaining to the firm's physical, digital, operational and administrative security.

12.2 Where necessary, the relevant aspects of the firm's security are updated to ensure that the strongest possible security measures are in place.

13. SUB-CONTRACTORS

13.1 There are a number of instances where the firm, with the prior consent of the client, must make use of a sub-contractor, for example, where mortgage documents must be signed in front of a non-employee of the firm.

13.2 Before the relevant documents are sent to the sub-contractor, electronically or in hard copy, the employee ensures that:

13.2.1 In the case of deeds/conveyancing matters: that the document/s only be sent to the client, or a practicing attorney who is on the panel of the bank concerned. Further, that the document is sent as near as possible to the residential or business address of the client, after the attorney has been contacted telephonically and enquiries made about their willingness to act as correspondent, their fee structure and an agreement from them that they will handle the documents and information in accordance with our privacy policy has been obtained; and

13.2.2 In the case of all other matters, including court process and documents: that these documents only be sent to the client, an officer of the court or a practicing attorney after the attorney has been contacted telephonically and enquiries made about their willingness to act as correspondent, their fee structure and an agreement from them that they will handle the documents and information in accordance with our privacy policy has been obtained.

13.3 Other sub-contractors are requested to undertake, in writing, to comply with our privacy and POPIA policies, and to sign a confidentiality agreement with the firm.

13.4 Where a sub-contractor handles client information in a manner contrary to the provisions of our privacy and POPIA policies, or there are reasonable grounds to believe that a sub-contractor has handled client information in a manner contrary to the provisions of our privacy and POPIA policies, this will be reported to the data subject concerned, as well as to the Information Regulator, by our Information Officer.

14. BACK-UP SUPPORT

14.1 All information stored on the main frame is automatically backed up on a daily basis;

14.2 The back-up hardware is kept in the firm's vault and is tested monthly by our IT agent to ensure that the information is properly stored; and

14.3 A further copy is kept at the offices of the firm's IT agent, in a locked cupboard (these copies are taken to the IT agent's office by the IT agent him-/herself, or where necessary, by an employee of the firm).