ATLANTIC BEACH

ATLANTIC BEACH HOMEOWNERS' ASSOCIATION POPIA MANUAL

MANUAL PREPARED IN ACCORDANCE WITH THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)

Homeowners' Association name: Atlantic Beach

Homeowners' Association *domicilium* address: Ground Floor Mandela Rhodes Place

Cnr Wale & Burg Streets

CAPE TOWN

8000

POPIA Information Officer name: Francois Pierre Swart

ATLANTIC BEACH

INDEX **PAGE**

ANNEXURES

ATLANTIC BEACH

Understanding the POPIA

1. **Purpose of the POPIA**

The purpose of the Protection of Personal Information Act is to protect the South African Constitutional right to privacy. This is done by regulating the processing of an individual's personal information to protect against its unlawful collection, use, disclosure and destruction. The personal information of owners, tenants, employees and trustees of a homeowners' Association (the Association) must be processed in accordance with the conditions for lawful processing, and the prescribed POPIA rights of these data subjects must be upheld.

2. **Terms used in the POPIA (S1 of the POPIA)**

2.1 Data subject – person to whom the personal information relates: ***the unit owner, tenant, service provider, trustee and employee.***

2.2 Information officer – the party responsible for ensuring that the Association complies with the conditions of POPIA;

2.3 Operator – the person who processes personal information for the Association**.**

2.4 Personal information – information relating to a person including, but not limited to, an ID number, email address, physical address, telephone number, bank details, biometric information, and private correspondence sent by that person.

2.5 Processing – activities concerning personal information which includes, but are not limited to, the collection, collation, retrieval, erasure, destruction and dissemination of personal information.

2.6 Responsible party – a party who processes personal information: ***the Association.***

2.7 Record – recorded information regardless of form or medium, in the possession of a responsible party**.**

2.8 Special personal information – information concerning religious/philosophical beliefs, race, ethnicity, trade union membership, political persuasion, health, sex life, biometric information, criminal behaviour of a data subject.

3. **Definitions**

a) "Association" means Atlantic Beach Homeowners Association;
b) "consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
c) "Constitution" means the Constitution, regulations and rules of the Association from time to time in force;
d) "Member" means every registered owner of an erf or residential section;

4. **Information held by the Association.**

The Association processes the personal information of owners, tenants, employees, directors, trustees, service providers, and suppliers for the proper governance and functioning of the scheme.

5. **The Association's POPIA obligations**

The Association must process personal information in accordance with the 8 conditions for lawful processing as prescribed in sections 8 to 25 of the POPIA **(Annexure A)**. These conditions impose the following obligations on the Association (not an exhaustive list):

i) The Association must obtain consent from a competent person if the data subject is under the age of 18 years;
ii) The Association must obtain consent for the processing of any special personal information;
iii) The Association must destroy records of personal information if it is no longer necessary to retain them for the purpose for which they were collected, or the period required by law;
iv) The Association must take steps to ensure the data subject is aware of their information being processed and the purpose for which it is being processed;
v) The Association must take technical and organisational security measures to protect the personal information held;
vi) The Association must maintain the safeguard measures, regularly verify that they are effectively implemented and continually updated;
vii) The Association must ensure any Operator maintains the Association's security measures;
viii) The Association must notify the Regulator and the data subject if there are reasonable grounds to believe there has been unauthorised access to information;
ix) The Association must provide confirmation of personal information held and a record thereof if requested by a data subject;
x) The Association must correct, delete or destroy personal information if reasonably requested by a data subject; and
xi) The Association must provide a record of all third-party access to personal information if requested by a data subject;

6. **Biometrics**

The Association processes biometric information in order to maintain the security of the Atlantic Beach Estate. Biometric information is classified as special personal information and constitutes a case where the Association must obtain the data subject's consent to process their biometric information. This consent need not be written but **Annexure F1** attached hereto may be used.

A record of data subjects' consent can be tracked using the register attached in **Annexure F2**.

7. **Direct Marketing**

The Association shall only be entitled to process personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, SMSs or e-mail if –

a) the data subject has given his, her or its consent to the processing; or
b) the data subject is a client of the Association,

provided that the data subject was given a reasonable opportunity to object, free of charge and with ease to such use of his details at the time when the personal information was initially collected; and on the occasion of each communication thereafter.

8. **The Information Officer**

The Association has appointed **Francois Pierre Swart** as the Information Officer and has completed registration with the Information Regulator in terms of the POPIA. The Information Officer is responsible for:

a) The encouragement of compliance with the conditions for the lawful processing of personal information;
b) Dealing with requests made to the Association pursuant to the POPIA;
c) Working with the Regulator in relation to investigations;
d) Otherwise ensuring compliance by the Association with the POPIA; and
e) As may be prescribed.

9. **Correction, Retention, and Destruction of Information**

Upon receiving a request from a data subject for the correction or destruction of information in accordance with **Annexure D2**, the Association must, as soon as reasonably practicable correct the information; or destroy or delete the information.

The Association shall provide the data subject, to his or her satisfaction, with credible evidence in support of the correction or deletion of the personal information; or where agreement cannot be reached between the Association and the data subject regarding the steps to be taken in respect of the correction or deletion of the personal information, the Association shall take such steps as are reasonable in the circumstances to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made. The data subject shall be informed in accordance with the form attached as **Annexure F**.

Notwithstanding anything to the contrary contained herein, personal information shall only be retained for so long as it is required by the Association to conduct its business or in terms of any applicable laws. The Association's retention policy is contained in **Annexure J** and may be amended or updated from time to time.

10. **Employee Use Policy and Security Measures**

Annexure K sets out the Association's security measures put in place to protect the personal information, as well as the Association's policy relating to the use of the Association's resources.

11. **Security Compromises**

The Association must have a contingency plan in the event of a security compromise. **Annexure L** contains the Association's procedures in the event of a security breach.

ANNEXURE A

Association Obligations – 8 Conditions for Lawful Processing

Condition 1

Accountability – The Association must ensure that it complies with these 8 conditions and all measures implemented to ensure the lawful processing of information at all times (S8);

Condition 2

Processing limitation – Personal information must be processed lawfully and in a reasonable manner that does not infringe on the data subject's privacy. Information must be processed in a manner that is adequate, relevant and not excessive. (S9 – S10)

The processing of personal information may only occur if:

a) the data subject, or a competent person if the data subject is under 18 years old, consents;
b) the processing is necessary to carry out the performance of a contract to which the data subject is a party;
c) the processing complies with an obligation imposed by law;
d) the processing protects a legitimate interest of the data subject;
e) processing is necessary for the performance of a public law duty by a public body; or
f) processing is necessary for the legitimate interests of the Association or a third party to whom the information is supplied. (S11)

A data subject has the right to object on reasonable grounds to the processing of their personal information and must do so in the prescribed manner using the prescribed form (Annexure D1). (S11)

Personal information must be collected directly from the data subject unless:

a) the information is derived from a public record or has been deliberately made public by the data subject;
b) the data subject has consented to the collection from another source;
c) the collection from another source would not prejudice a legitimate interest of the data subject;
d) the collection from another source is necessary for the reasons states in S12(2)(d) of the POPIA;
e) collection directly from the data subject would prejudice a lawful purpose; or
f) collection directly from the data subject is not reasonably practicable in the circumstances. (S12)

Condition 3

Purpose specification – Personal information must be collected only for a specific, explicitly defined lawful purpose related to the function or activity of the Association, and a data subject must be aware of this purpose. (S13)

Records of personal information must not be retained longer than necessary to achieve the purpose for which the information was collected, unless:

a) the retention of the record is required by law;
b) the Association requires a record to carry out lawful functions or activities;
c) the retention of the record is required by a contract between the Association and the data subject;
d) the data subject has consented to the retention.

Records of personal information must be destroyed as soon as reasonably practicable after the Association is no longer authorised to retain the information. (S14)

Condition 4

Further processing – The further processing of personal information by the Association must be compatible with the purpose of collection. To assess whether further processing is compatible, the Association must:

a) assess the relationship between the purpose of the further processing and the purpose for which the information was originally collected;
b) assess the nature of the information in question;
c) assess the consequences of further processing for the data subject;
d) assess the manner in which the information has been collected; and
e) assess any contractual rights and obligations between the Association and the data subject. (S15)

Condition 5

Information quality – The Association must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary (S16);

Condition 6

Openness – The Association must maintain documentation of the processing activities regarding personal information, including receipt, recording, organisation, cancellation, storage and use as well as transmission, re-formatting, merging and destruction. (S17)

The Association must take reasonably practicable steps to ensure that the data subject is aware of their information being collected, the purpose for the collection and any further information necessary. (S17-S18);

Condition 7

Security safeguards – The Association must secure the integrity and confidentiality of the personal information by taking reasonable technical and organisational measures to prevent loss, damage, unauthorised destruction as well as unlawful access. This must be done by identifying all risks to personal information and subsequently establishing, monitoring and updating appropriate safeguards against these risks. (S19)

Any operators processing on behalf of the Association must only process personal information with the knowledge or authorisation of the Association, or if it is required by law. The operators must treat all personal information as confidential. (S20)

There must be a written contract between the Association and the operator confirming that the operator will process personal information in accordance with the Association's S 19 security measures. The operator also has a duty to notify the Association immediately if there are reasonable grounds to believe that there has been unauthorised access to or acquisition of personal information. The Association then has the duty to notify the data subject as well as the Regulator. (S21 – S22)

Condition 8

Data subject participation – The data subject has the right to request the Association to advise whether or not they hold personal information relating to the data subject, and to request the record of the personal information within a reasonable time and at the prescribed free (S23-24).

ATLANTIC BEACH

ANNEXURE B

NOTIFICATION OF DATA SUBJECTS' RIGHTS IN TERMS OF S5 OF THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013 (POPIA)

Rights of Data Subjects (S5 of the POPIA)

Data subjects have the right to:

1. Have their personal information processed in accordance with the POPIA conditions for lawful processing;
2. Be notified that personal information about them is being collected;
3. Be notified that personal information has been accessed or acquired by an unauthorised person;
4. Establish whether the Association holds their personal information and to request access to it;
5. Request, where necessary, the correction, destruction or deletion of their personal information;
6. Object on reasonable grounds to the processing of their personal information;
7. Object to the processing of their personal information for purposes of direct marketing;
8. Not have their personal information processed for purposes of direct marketing;
9. Not be subjected to a decision based solely on the automated processing of their personal information;
10. Submit a complaint to the Information Regulator regarding interference with the protection of their personal information;
11. Institute civil proceedings regarding interference with their personal information.

Processing of Data Subject's Personal Information (S5 of the POPIA)

The data subject is hereby informed that personal information about them is being collected and processed in accordance with the POPIA. The Association is obligated by the Companies Act and its Constitution to process information for the proper functioning and governance of the scheme.

ANNEXURE C

FORM FOR THE ASSOCIATION TO RECORD ACCESS TO DATA SUBJECT'S INFORMATION (S23 OF THE POPIA)

The data subject has the right to request the Association to:

1. Advise, free of charge, whether it holds the data subject's personal information;
2. Provide the record or a description of the personal information held;
3. Provide information about the identity of all third parties who have had access to the personal information;
4. In terms of S23(1)(b)(2) of the POPIA, the data subject making a request in terms of 2 and 3 above will be required to pay a prescribed fee to the Association, at the rate determined by the PAIA.

Third party access record in terms of S23 of the POPIA				
Date	Data subject unit number	Third party name	Personal information provided	Reason for provision of information

ATLANTIC BEACH

ANNEXURE D1 – Form 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3)(a) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[REGULATION 2]

Note:

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

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

ATLANTIC BEACH

C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) TO (f) (*Please provide detailed reasons for the objection)*

Signed at _____this _____day of _____

_____

Signature of data subject/designated person

ATLANTIC BEACH

ANNEXURE D2 – Form 2

REQUEST FOR CORRECTION/DELETION OF PERSONAL INFORMATION OR DESTRUCTION/DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[REGULATION 3]

Note:

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

Mark the appropriate box with an "X".

Request for:

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

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

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

C	INFORMATION TO BE CORRECTED/DELETED/DESTROYED
D	REASONS FOR CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS ON SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. *(Please provide detailed reasons for the request)*

Signed at _____this _____day of _____

_____

Signature of data subject/designated person

ATLANTIC BEACH

ANNEXURE E

NOTIFICATION TO DATA SUBJECT THAT PERSONAL INFORMATION HAS BEEN CORRECTED, DELETED OR DESTROYED AS PER A REQUEST IN TERMS OF S24(4) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013 (POPIA)

To _____ Date ____/____/_____

Notification to Data Subject in terms of S24(4) of the POPIA

This note serves to inform you that the personal information you requested to be corrected/deleted or destroyed has been corrected/deleted or destroyed.

The changes have been recorded in the attachment hereto.

_____

Signed by the Information Officer on behalf of the Association

ATLANTIC BEACH

ANNEXURE F1

BIOMETRICS CONSENT FORM IN TERMS OF S26 OF THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013 (POPIA)

I, the undersigned _____(full name), Unit Number _____by my signature below give consent to the Association to process my biometric information.

_____ ____/____/_____

Signature Date

GUARDIAN'S CONSENT

If the data subject above is under the age of 18, a competent person must give consent in terms of S35 of the POPIA.

I, the undersigned _____(full name), Unit Number _____by my signature below give consent to process the biometric information of _____.

_____ ____/____/_____

Signature Date

ATLANTIC BEACH

ANNEXURE F2

SCHEME BIOMETRICS CONSENT REGISTER (S26 AND S27 OF THE POPIA)

Scheme Biometrics Consent Register				
OCCUPIERS				NON-OCCUPIERS
Scheme Unit No.	Owner Code	Tenant Code	Employee Code	Trustee Code

ATLANTIC BEACH

ANNEXURE G

AUTHORISATION OF THE INFORMATION OFFICER

(In terms of the Promotion of Access to Information Act 2 of 2000)

I, the undersigned, _____(full name of the default Information Officer) hereby appoint _____(full name of authorised Information Officer) to be the Information Officer of _____(insert BC/HOA name), and authorise _____(full name of authorised Information Officer) to exercise any of the powers, duties and responsibilities conferred or imposed on me by the Protection of Personal Information Act, 2013 and the Promotion of Access to Information Act, 2000.

I reserve my right to exercise any of the powers, duties and responsibilities conferred herein, as well as the right to amend and/or withdraw any of those powers, duties and responsibilities.

_____ _____

Default Information Officer (name) Signature

By my signature herein below, I hereby accept the authorisation to be the Information Officer of the above-mentioned scheme.

_____

(Full name of authorised Information Officer)

Date: _____

ATLANTIC BEACH

ANNEXURE H

DESIGNATION AND DELEGATION OF AUTHORITY TO THE DEPUTY INFORMATION OFFICER

(In terms of section 56 of the Protection of Personal Information Act No. 4 of 2013 (POPIA) and section 17(1) of the Promotion of Access to Information Act No. 2 of 2000 (PAIA).

I, the undersigned, _____(full name of Information Officer) hereby designate _____(full name of person being designated) as the/a Deputy Information Officer of (insert BC/HOA name), the Responsible Party.

Furthermore, I hereby delegate to you the following powers, duties and responsibilities, as conferred or imposed on me by POPIA and PAIA, specifically all the duties required of the responsible officer as set out in par 6 of the Guidance Note on Information Officers and Deputy Information Officers issued by the Information Regulator on 01 April 2021.

Please be advised that I reserve the right to exercise any of the powers, duties and responsibilities conferred herein, as well as the right to amend and/or withdraw any of those powers, duties and responsibilities.

_____

Information Officer
(Name and signature)

By my signature herein below, I hereby accept the delegation and designation as the Deputy Information Officer.

_____

(Name of designate)

Date: ____/____/_____

ANNEXURE I

AGREEMENT IN RESPECT OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

We confirm that _____(insert service provider's name), the Operator, processes personal information on behalf of _____(insert HOA name), the Responsible Party.

1. "Personal information" shall have the meaning ascribed to it as in the Protection of Personal Information Act (POPIA).
2. The Operator hereby undertakes as follows:
   2.1 The Operator will secure the integrity and confidentiality of the personal information provided by the Responsible Party. This will be done by taking appropriate, reasonable technical and organisational measures to prevent the:
      2.1.1 loss of, damage to or unauthorised destruction of personal information; and
      2.1.2 unlawful access to or processing of the personal information.
   2.2 In furtherance of the obligation set out in clause 2.1 above, the Operator will undertake reasonable measures to:
      2.2.1 identify all reasonably foreseeable internal and external risks to the personal information in its possession or under its control;
      2.2.2 establish and maintain appropriate safeguards against the risks identified in terms of clause 2.2.1 and any security measures established by the Responsible Party;
      2.2.3 regularly verify that the safeguards established in terms of clause 2.2.2 are effectively implemented;

2.2.4 ensure that the safeguards established in terms of clause 2.2.2 are continually updated in response to new risks or deficiencies in previously implemented safeguards;

2.2.5 have due regard to generally accepted information security practices and procedures applicable or required in terms of specific industry or professional rules and regulations;

2.2.6 process personal information only with the knowledge or authorisation of the Responsible Party;

2.2.7 notify the Responsible Party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

3. The Responsible Party confirms that it authorises the Operator to process personal information, provided by the Responsible Party, on the Responsible Party's behalf.

Name: _____

Title: _____

Who warrants their authority for:

_____

(insert service provider's name)

Signature: _____

Name: _____

Title: Information Officer of HOA

Signature: _____

ANNEXURE J

RETENTION POLICY

Record type	Record description	Retention period	Considerations
Accounting / Financial	Annual audit records	7 years post audit	SARS requirements and standard practice
	Financial Statements	7 years	SARS requirements and standard practice
	Bank Statements	7 years	SARS requirements and standard practice
	Tax invoices	7 years	SARS requirements and standard practice
	Payroll	10 years	Basic Conditions of Employment Act Unemployment Insurance Act
Emails	Routine business emails not concerning any documents or records referenced elsewhere herein	90 days on computer then archived for 3 years prior to destruction.	
	Emails concerning or containing any of the documents or records referenced elsewhere	See subject matter for retention period	Consider whether it contains personal information
	Personal emails sent or received on the Association's systems and NOT concerning any Association matter or affairs or any matter not referenced herein	Keep hardcopy for 1 year – delete electronic version on same day basis except if they concern any legal dispute or issues concerning the Association or management – then see information officer	
Marketing	Email lists	Should only be kept as long as it is necessary to achieve the purpose for which it was collected, BUT if person asks to be unsubscribed, must remove them immediately, free of charge	POPIA

Record type	Record description	Retention period	Considerations
	Marketing Material	3 years from date of publication	Not required in terms of Consumer Protection Act but is advised
Members	Member information	7 years	Income Tax Act and Community Schemes Management Act
Tax Filings	SARS Tax returns and supporting documents	5 years from date of submission	5 years from date of submission of return (Income Tax Act and Value-Added Tax Act), provided, if documents concern any audit or legal proceedings, then 5 years from final resolution of audit or proceeding.
Legal	Commercial agreements	5 years after termination	
	Insurance Policies	5 years after termination	
	Minutes of trustee meetings	Indefinite	
	Documents sent to members	Indefinite	
	Legal processes	5 years	
	Legal Opinions	Indefinite	
	Intellectual property filings and documentation	Patents: 20 years, then have to renew, so recommended to keep all documents until need to renew again. Trademarks: keep all documents permanently. Copyright: keep all documents permanently	
Human Resources	CVs and background checks	3 years if appointed. Delete immediately if not appointed, alternatively 1 year if to be considered for future consideration	Basic Conditions of Employment Act
	Employment agreements	4 years after termination	Basic Conditions of Employment Act
	Disciplinary records	3 years after termination	Labour Relations Act does not provide a retention period, only states that

Record type	Record description	Retention period	Considerations
			records should be kept. Recommended: 3 years
	Termination records and resignations	3 years after termination	Labour Relations Act does not provide a retention period. Recommended: 3 years
	Performance reviews and promotion records	3 years after termination	Basic Conditions of Employment Act
	General employee records	5 years	Income Tax Act Employment Equity Act Compensation for Occupational Injuries and Diseases Act Note: this is the longest retention period in respect of employees
	Staff manuals and policies	Indefinite	

NOTES

1. Tax Records

Tax records include, but may not be limited to, documents concerning payroll, expenses, proof of deductions, business costs, accounting procedures, and other documents concerning the Association's revenues.

2. Employment Records/Personnel Records

In the event that a past or present employee files as a complaint to the CCMA (in respect of the Labour Relations Act), or legal action against the Association for employment practices, all employment documents for that employee should be retained for the duration of that action.

3. Press Releases

The Association should retain permanent copies of all press releases and publicly filed documents to test the accuracy of any document a member of the public can theoretically produce against the Association.

ANNEXURE K

EMPLOYEE USE POLICY AND SECURITY MEASURES

1 General Use

1.1 Employees must lock unattended devices when leaving the work area and any portable electronic devices containing personal information should be securely stored.

1.2 Employees may only connect or install computer hardware and software owned by and installed by the Association on its equipment or network.

1.3 All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Association are the property of the Association, unless otherwise agreed by the Association in writing.

2 Portable Media Devices

2.1 Employees must ensure that all external or portable media devices are be scanned for virus infections prior to connecting to or copying information to an Association computer or network.

2.2 Employees may not store personal information on portable media devices.

2.3 Employees must report loss of portable devices to the Information Officer.

2.4 Employees must ensure that portable media devices are wiped clean of all data if no longer in use. All external media must be sent to the Association's IT personnel to ensure the correct processes are followed.

3 Mobile devices

3.1 Employees occasionally have access to email and other work-related applications on their personal mobile devices.

3.2 The Association shall ensure that such access is revoked when the employee leaves the employ of the Association.

3.3 Employees must make use of two-factor authentication in order to access emails from a mobile device and such mobile device must have adequate protection from use of third parties in the form of passwords or fingerprint/facial recognition.

4 Prohibited Activities

Employees may not -

4.1 deliberately crash an information system. If a crash occurred because of user action, a repetition of the action by the employee may be viewed as a deliberate act;

4.2 attempt to break into an information resource or to bypass a security feature;

4.3 introduce, or attempt to introduce, computer viruses, trojan horses, peer-to-peer or other malicious code into an information system unless specifically authorised in writing by the Information Officer;

4.4 wilfully access or inspect confidential or sensitive information which is not authorised or approved on a "need to know" basis.

5

6 Monitoring

6.1 Generally, while it is not the policy of the Association to monitor the content of any electronic communication, the Association is responsible for servicing and protecting its equipment, networks, data, and resources and therefore may be required to access electronic communications of employees from time to time.

6.2 Employees should structure all electronic communication with recognition of the fact that the content could be forwarded, intercepted, printed, or stored by others.

7 Security Policy

7.1 The Association takes appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information.

7.2 In this regard the Association –

7.2.1 employs data security technology to secure the personal information and protect it against threats;

7.2.2 limits access to personal information to those employees who require access for the purpose of performing their obligations; and

7.2.3 requires employees to sign confidentiality agreements or employment agreements which include confidentiality undertakings.

7.3 Each employee must comply with the safety and security measures of the Association when processing personal information.

7.4 The Association will continuously review its security controls and processes to ensure that all personal information is secure.

8 Virus Protection

8.1 Employees may not stop the update process for virus protection as it is critical to the security of all data and must be allowed to complete. Virus protection software must be installed on all Association resources.

8.2 Should an employee disable a virus scanner or firewall, it will be viewed in a serious light and may lead to disciplinary procedures being instituted against the employee.

9 Identification and Authentication

9.1 Access to the Association's networks shall be subject to authorisation and authentication by an access control system.

9.2 Along with the user IDs, passwords are required to gain access to the Association's systems. All passwords are restricted by a password policy to be of a "strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

10 Malicious Code

10.1 The Association will maintain a record of virus patterns for all computers and servers on the Association's network. Appropriate IT personnel are responsible for providing reports for emergency situations, as requested by the Association.

10.2 Prior to the installation of any new software on Association resources, the software will be tested by appropriate IT personnel to ensure compatibility with currently installed software and network configuration. In addition, IT personnel must scan all software for viruses before installation.

ANNEXURE L

SECURITY COMPROMISES AND CONTINGENCY PLANS

1 Contingency Plan

1.1 The Association is committed to maintaining formal processes for responding to an emergency or other occurrence that damages systems containing personal information. The Association shall continually assess potential risks and vulnerabilities to protect information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

1.2 The Association's IT personnel shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

1.3 All servers shall be backed up daily and server backups shall be kept for 30 days and shall be stored in a secure access-controlled data centre.

1.4 Backup procedures shall be tested monthly to ensure that exact copies of information can be retrieved and made available. Such testing shall be documented by IT personnel. To the extent such testing indicates need for improvement in backup procedures; the IT personnel shall identify and implement such improvements in a timely manner.

2 Disaster Recovery Plan

2.1 The Information Officer shall be responsible for developing and regularly updating the written disaster recovery plan for the Association for the purpose of:

2.1.1 restoring or recovering any loss of information and/or systems necessary to make information available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

2.1.2 continuing operations during such time information systems are unavailable.

2.2 Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored.

2.3 The disaster recovery plan shall include the following -

2.3.1 A current copy of the written backup procedures developed and updated pursuant to this policy.

2.3.2 The members of an emergency response team, which team shall be responsible for the following -

2.3.2.1 determining the impact of a disaster and/or system unavailability on operations;

2.3.2.2 securing the site and providing on-going security;

2.3.2.3 retrieving lost data;

2.3.2.4 identifying and implementing appropriate "work-arounds" during such time information systems are unavailable;

2.3.2.5 taking such steps necessary to restore operations;

2.3.2.6 telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster.

2.4 The disaster recovery team shall meet on at least an annual basis to -

2.4.1 review the effectiveness of the plan in responding to any disaster or emergency experienced by the Association; and

2.4.2 review the written disaster recovery plan and make appropriate changes to the plan.

3 Reporting Software Malfunctions

3.1 In the event that an employee's software does not appear to be functioning correctly, the employee should inform the appropriate IT personnel without delay as the malfunction - whether accidental or deliberate - may pose a security risk.

3.2 If an employee suspects a computer virus infection, the employee must -

3.2.1 immediately stop using the computer;

3.2.2 not carry out any commands, including commands to 'save' data;

3.2.3 not close any of the computer's windows or programs;

3.2.4 not turn off the computer or peripheral devices;

3.2.5 if possible, physically disconnect the computer from networks to which it is attached;

3.2.6 inform the appropriate IT personnel as soon as possible;

3.2.7 write down any changes in hardware, software, or software use that preceded the malfunction; and

3.2.8 not attempt to remove a suspected virus.

4 Report Security Incidents

4.1 Employees are responsible for the day-to-day, hands-on security of the resources that they use and must formally report all security incidents or violations immediately to the Information Officer.

4.2 Reports of security incidents shall be escalated as quickly as possible. Each incident will be analysed to determine if changes in the existing security structure are necessary.

4.3 All reported security incidents shall be logged, and the remedial action indicated. It is the responsibility of the Information Officer to provide training on any procedural changes that may be required because of the investigation of an incident.

5 Internal Breach Notification Procedures

5.1 Containing the Breach: In the event of a security breach, the following steps shall be taken to limit the scope and effect of the breach:

5.1.1 stopping the unauthorised practice;

5.1.2 recovering the records, if possible;

5.1.3 shutting down the system that was breached;

5.1.4 mitigating the breach, if possible; and

5.1.5 correcting weaknesses in security procedures and systems.

5.2 Investigating the Breach

5.2.1 To determine what other steps are immediately necessary, the Information Officer will investigate the circumstances of the breach.

5.2.2 The Information Officer will review the results of the investigation to determine root cause(s), evaluate risks, and develop a resolution plan.

5.3 Prevention

5.3.1 If the Information Officer determines that it is necessary, a full security audit of physical, organisational, and technological measures will be conducted.

5.3.2 Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.

6 External Notification of Security Compromise

6.1 Where there are reasonable grounds to believe that the personal information has been accessed by any unauthorised person, the Association will notify –

6.1.1 the information regulator;

6.1.2 the data subject is affected by the security compromise unless the identity of the data subject cannot be established; and

6.1.3 the South African Police Service, in the event that criminal activity is suspected.

6.2 The notification must be made as soon as reasonably possible after the discovery of the compromise, considering 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 Association's information system.

6.3 The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including –

6.3.1 a description of the possible consequences of the security compromise;

6.3.2 a description of the measures that the Association intends to take or has taken to address the security compromise;

6.3.3 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

6.3.4 if known to the Association, the identity of the unauthorised person who may have accessed or acquired the personal information.