POLICY PREPARED IN ACCORDANCE WITH SECTION 51 of THE PROMOTION OF ACCESS TO INFORMATION ACT 2/2000 AND THE PROTECTION OF PERSONAL INFORMATION ACT 4/2013

for

CHRISTIAN SEAMAN'S ORGANISATION

Introduction

This Policy (or *the* policy) was developed to provide clear guidance to all Christian Seamans' Organisation (CSO) employees and to ensure strict adherence to the law. The CSO is a voluntary association of persons conducting missionary work in the harbors of South Africa.

Inherent in the aforementioned mission, CSO has access to and needs to process personal data and information relating to individuals. This policy sets out how such personal data shall be processed, handled and stored to meet the data protection standards of CSO and to comply with the legal standards governing its clients and the legislation in South Africa, as well as setting out the process for obtaining access to records held by the CSO as envisaged in our legislation.

This policy seeks to ensure that CSO:

i. Promotes access to information, to relevant persons in the applicable circumstances and on the basis as provided for in terms of the legislation of the Republic of South Africa;
ii. Complies with international legal standards and best practice for the receipt, importing, processing, handling and storing of personal data of individuals ("data subjects");
iii. Protects the rights of its clients and third parties in respect of individuals' data, transparently renders how it process, handles and stores individuals' data and protects itself from the risks of a data breach.

PROMOTION OF ACCESS TO INFORMATION ACT

Part I

(Information required under Section 51(1)(a) of the Act)

Name of Body: **CHRISTIAN SEAMAN'S ORGANISATION**
Physical Address: **MILPARK 303, IXIA STREET**
MILNERTON, 7400
Postal Address: **Private Bag X09, MILNERTON, 7435**
Head of Body: **E WEIDEMAN**
Telephone No: **021-551 2694**
Cell Phone No: **071 279 3061**
Email: cso@mweb.co.za

Part II
(Information required under Section 51(1)(b) of the Act)

A guide on how to use the Act is to be compiled by the Human Rights Commission in terms of Section 10 of the Act by no later than August 2003. Any queries should be directed to:

The South African Human Rights Commissioner:
PAIA Unit, The Research and Documentation Department
Postal address: Private Bag 2700
Houghton, 2070
Telephone: +27 11 484 8300
Fax: +27 11 484 0582
Website: www.sahrc.org.za
E-mail: PAIA@sahrc.org.za

Part III
(Copy of notice, if any, required under section 51(1)(c) of the Act)

Currently not applicable

Part IV
(Information required under Section 51(1)(d) and (e) of the Act)

For the purposes of this manual and the Act, the records held by CSO are categorised by the nature of the content thereof as follows:

4.1 Records kept in accordance with other legislation but not limited to:

- Basic Conditions of Employment Act 75 of 1997;
- Deeds Registries Act 47 of 1937;
- Employment Equity Act 55 of 1998;
- Income Tax Act 58 of 1962;
- Labour Relations Act 66 of 1995;
- Medical Schemes Act 131 of 1998;
- Pension Funds Act 24 of 1956;
- Regional Services Councils Act 109 of 1985;
- Skills Development Levies Act 9 of 1999;
- Stamp Duties Act 77 of 1980;
- Unemployment Insurance Act 63 of 2001

The above records which are of public nature are available automatically without a person having to request access thereto in terms of the Act, as envisaged in Section 52.

4.2 Records relating to the marketing documentation, brochures, newsletters and official letters to donors requesting support of CHRISTIAN SEAMAN'S ORGANISATION.

4.3 Records and correspondence between persons within and without the company, e.g. internal written departmental memos and minutes for meetings:

internal telephone lists, address lists, company policy documents, supplier contracts, employee records, accounting and banking records, insurance policies, documentation; policies relating to investments, documentation relating to SARS income tax exemption, documents relating to motor vehicles owned, necessary permits and licences, title deeds in respect of the properties at 303 Milpark, Ixia Street, Milnerton and Mia Lab Mansions 2, Claribelweg 85, Morningside, Durban.

4.4 The website address of CHRISTIAN SEAMAN'S ORGANISATION is www.cso.co.za and is accessible to anyone who has access to the internet. The website contains information in various categories to the company and its contact particulars.

The Request Procedure

I Form of Request

- The requester must have the prescribed form being Schedule 1 hereto to make request for access to a record. This must be made to the head. This request must be made to the address or electronic mail address of CHRISTIAN SEAMAN'S ORGANISATION.

- The requester must provide sufficient detail on the request form to enable the head to identify the record and the requester. The requester should also indicate which form of access is required and specify a postal address or fax number in the republic. The requester should also indicate if, in addition to a written reply, any other manner is to be used to inform the requester and state the necessary particulars to be so informed.

- The requester must identify the right that is sought to be exercised or protected and provide an explanation of why the requested record is required for the exercise or protection of the right.

- If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the head.

II Fees

A requester who seeks access to a record containing personal information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee:

- The head must by notice require the requester (other than a personal requester) to pay the prescribed request fee (if any) before further processing the request;

- The fee that the requester must pay is R50.00. The requester may lodge an application to the Court against the tender of payment of the request fee

- After the head has made a decision on the request, the requester must be notified in the required form

- If the request is granted then a further access fee must be paid for reproduction and for search and preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure

Part V
(Other information as may be prescribed required under section 51(1)(f))

The Minister of Justice and Constitutional Development has not made any regulations in this regard.

Part VI
(Availability of manual under Section 51(3))

An unabridged version of this manual is available for inspection by the general public upon request, from the South African Human Rights Commission;

Part VII
(Prescribed form and fee structure in respect of private bodies)

The forms and fee structure prescribed under the Act are available at the website of the Department of Justice and Constitutional Development (www.doi.gov.za) under the "regulations" section as well as the SAHRC website (www.sahrc.org.za).

PROTECTION OF PERSONAL INFORMATION ACT

Legislative Environment
This policy seeks to align best practice in CSO with legal standards governing its clients and its services, and including particular legislation such as the Protection of Personal Information Act ("POPI").

Scope and Application
This policy applies to all employees of CSO in respect of all personal data processed and accessed in the provision of services by CSO to its clients, in particular data that it holds relating to identifiable individuals, including, but not limited to the following:

- names of individuals;
- physical and postal addresses;
- email details;
- all telephone and mobile phone numbers;
- all social media tags and identifiers;

- all data and information relating to an individual or received from a client in the course of providing services to such client; and/or
- all data of a data subject protected for the benefit of such individual in terms of POPI, or sought to be protected by the latter statute.

This policy governs every employee of CSO both during the course of his/her services to it, and to the extent applicable, after termination of services. To the extent that this policy sets out workplace rules governing the employee in the course of his/her work and services to CSO, it shall form part of the CSO workplace rules/procedure and is hereby also incorporated into it. A breach of any rule in relation to the protection of personal data set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal. The imposition of any disciplinary sanction or dismissal shall not preclude the company from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations.

Protection

This policy seeks to protect CSO from various data security risks including: breaches of confidentiality through data breaches, hacking risks, and the risks of liability in relation to its clients and third party's data acquired from such clients. The rules and standards set out in this policy apply regardless of whether personal data relates to a client or to another third party and/or is stored electronically, digitally, on paper, or on other materials, or through other methods.

General rules relating to Personal Data

Personal data shall at all times be:

- processed fairly and lawfully, in accordance with legal standards applicable to such data or data categories;
- obtained only for specific lawful purposes;
- adequate, relevant and not excessive;
- accurate, and kept up to date;
- held for no longer than necessary for the purpose it was obtained for;
- processed in accordance with the rights of data subjects;
- be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically;
- not be disclosed or transferred or exported illegally, or in breach of any agreement with a client.

Responsible Parties

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

The Risk and Compliance Manager

The Risk and Compliance Manager is identified to all staff and is _____, who shall be registered as the responsible officer under POPI, and shall:

execute, and bear responsibility for reporting to executive management about compliance with all technological and operational data protection standards and protocols, and advise of any risk of breach at the earliest opportunity with a view to avoiding any risk or breach, or limiting any damage resulting from it. To ensure compliance with this provision,

- a Breach Notification Form must be completed by any employee of CSO who becomes aware of any breach /or possible breach;
- ensure that all operational and technological data protection standards are complied with;
- arrange data protection training and provide advice and guidance to all employees;
- be entitled and have authorisation to initiate disciplinary proceedings against any employee who at any time breaches any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) applicable in any department or area of the operations of CSO;
- review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;
- attend to requests from individuals to access data CSO holds about them ("data subject requests").

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for the performance of their service to CSO. Under no circumstances will data or personal information be shared outside the scope of required work outputs, or informally. In the event of any doubt, an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary. To ensure the aforegoing:

- Only identifiable, reputable and pre-authorised agents and subcontractors may be used;
- All employees must use a "POPI" form to advise the data subject/individual as to how CSO or a third party uses their personal information;
- Employees should keep all data secure, by taking sensible precautions and following the guidelines herein;
- In particular, strong passwords must be used and they should never be shared;
- Personal data should not be disclosed to unauthorised people, either within the company or externally;
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of; and,
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Direct marketing activities

Direct marketing is considered to be a legitimate business interest globally and in South Africa. POPIA imposes certain rules in relation to direct electronic marketing practices.

Section 69 of the POPI Act outlaws direct marketing by means of any form of electronic communication **unless** the Data Subject has given their consent for such. Such electronic communications includes:

- Emails;
- Smses;
- Automated call machines; and,
- Communication via any social media platforms.

A new data subject may only be approached **once**. In the event that consent is refused, it is refused forever. In the event that the data subject is an existing client or donor, the direct marketing by means of electronic communication may relate only to the CSO's own similar products or services and the data subject **must** have been given the right to opt out at the time that the information is collected and each time such communication is sent.

Data Storage

Where data is stored on paper, it must be kept in a secure and separate place where an unauthorised person cannot access or see it. This also applies to data stored electronically which has been printed out. When not required, such papers should be kept in a locked drawer, safe or cabinet. Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, and all unwanted paper must be shredded.

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

- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- Where data is stored on removable media such as a CD or a DVD these must at all times be locked away securely when not in immediate use;
- All data will only be stored on designated drives and servers and shall only be uploaded to approved cloud computing services;
- All servers containing personal data will be located in secure protected locations away from general office space;
- Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the Risk and Compliance Officer. The Risk and Compliance Manager will be responsible to schedule a minimum of two random tests each year;
- Data will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;

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

Data Use

Personal data is itself of little or no value to CSO unless the business can make use of it. It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended;
- Personal data should not be shared informally. In particular, it should never be sent by email without protection with appropriate passwords;
- The IT service provider / manager should be approached to explain how to send data to authorised external contacts to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties; and,
- Personal data shall never be transferred or sent to any entity not authorised directly to receive it.

Data Accuracy

The law requires CSO to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data Subject Access Requests

Where a client or individual who is entitled to it contacts the company requesting his/her personal information, it is called a "subject access request". Individuals who are the subject of personal data held by CSO are entitled to:

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

Subject Access Requests shall be made by e-mail and addressed to the Risk and Compliance Manager, who shall address it in consultation with management. The identity of a person making a data subject request will always be verified before handing over any information requested.

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

IT SHALL BE THE RESPONSIBILITY OF EVERY EMPLOYEE TO FAMILIARISE THEMSELVES WITH THE CONTENT OF THIS POLICY AND TO REMAIN UP TO DATE AS TO ANY CHANGES HERETO ISSUED IN WRITTEN FORM BY CSO.