EAST STREET, PO BOX 40, LINMEYER, 2105 ✝ TELEPHONE: PRIMARY: 011 435 0646/7/8 - HIGH: 011 435 1100 ✝ FAX, PRIMARY: 011 435 1708 - HIGH: 011 435 5886

Information Security Policy

1. SCHEDULE

1.1	The Organisation	Marist Brothers Linmeyer
1.2	Registration number	465-468-NPO
1.3	VAT registration number	
1.4	Physical address	East Street, Linmeyer
1.5	Email address	twilliams@maristbl.co.za; flawrence@maristbl.co.za

2. INTRODUCTION

2.1. All organisations that process any information that identifies an individual or juristic entity must implement information security measures.

2.2. Information security measures that are implemented will depend on the type of information that is processed. Information security measures effectively mean the processes and methodologies that are designed and implemented by an organisation to protect (i) printed, (ii) electronic, and / or (iii) any other form of sensitive or confidential information ("**Confidential Information**") and / or Personal Information (as defined below) from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

2.3. This policy and procedure document ("**Policy**") regulates the information security measures implemented by the Organisation set out in item 1.1. of the Schedule ("**Organisation**").

2.4. Where the information being processed comprises personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 ("**Personal Information**"), the provisions of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") will apply to the processing of such information by or on behalf of the Organisation.

3. OBJECTIVE

The objective of this Policy is to (i) regulate and formalise the information security environment of the Organisation, (ii) set out the various responsibilities of persons in the information security environment, and (iii) reference the related policies and procedures that will assist in improving information security in, or in relation to, the Organisation. It is important to ensure that information security measures address the confidentiality, integrity and availability of information.

4. SCOPE

This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Organisation's systems ("**Users**") that create and / or use records that relate to the Organisation's business operations.

5. TERMS AND ABBREVIATIONS

5.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Organisation makes use of the following terms:

5.1.1. "**ISO27000 Series**" means the international standard for implementing an information security management system; and

5.1.2. "**GDPR**" means the general data protection regulation of the European Union.

5.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

6. DOCUMENTS

6.1. This Policy should be read in conjunction with the following related policies and procedures of the Organisation, and any other policies and procedures that regulate data protection that the Organisation may implement in the future:

6.1.1. Acceptable Use Policy;

6.1.2. Access Management and Control Policy and Procedure;

6.1.3. Backup and Restoration Policy and Procedure;

6.1.4. Bring Your Own Device Policy;

6.1.5. Clean Desk and Clear Screen Policy;

6.1.6. Information Incident Management Policy and Procedure;

6.1.7. Information Privacy Policy and Framework;

6.1.8. Information Transfer Policy and Procedure;

6.1.9. Information Quality Policy;

6.1.10. Physical and Environmental Security Policy and Procedure;

6.1.11. Retention and Destruction Policy; and

6.1.12. Vulnerability and Penetration Testing Policy.

7. POLICY

7.1. The Organisation will apply the measures necessary to ensure the confidentiality, integrity and availability of (i) Confidential Information, and / or Personal Information. The Organisation will apply the ISO27000 Series in, or in relation to, its business practices.

7.2. The Organisation will further identify Personal Information and ensure that the information is protected in accordance with the requirements required by POPIA and / or the GDPR (if applicable).

7.3. Where the Personal Information in question is more sensitive in nature, such as information pertaining to minors, health and sex life ("**Special Personal Information**"), the Organisation will ensure that any more stringent measures required under POPIA and / or the GDPR in relation to the processing of such information are implemented.

8. RESPONSIBILITIES IN RELATION TO INFORMATION SECURITY

8.1. The various responsibilities in terms of this Policy must be allocated throughout the Organisation and Users will be categorised as follows:

8.1.1. **Accountable**: a User who will be ultimately accountable in the event of a breach or contravention of this Policy;

8.1.2. **Responsible**: a User who is responsible for the management and implementation of this Policy;

8.1.3. **Supportive**: a User who assists in implementing this Policy;

8.1.4. **Consulted**: a User who is consulted for advice and information regarding this Policy; and

8.1.5. **Informed**: a User who must and will be informed and given information regarding this Policy.

8.2. The responsibilities in terms of this Policy must be formalised in a (i) Responsible, (ii) Accountable, (iii) Supporting, (iv) Consulted and (v) Informed ("**RASCI**") Matrix and must be written into the job descriptions and / or contractual obligations, as the case may be, of the individual Users.

9. RIGHTS RESERVED BY THE ORGANISATION

The Organisation reserves the right to monitor, audit, screen, and preserve Organisation information as the Organisation deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Organisation information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Organisation. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Organisation, which may lead to further disciplinary action being taken.

10. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Organisation's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Organisation, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Organisation's disciplinary code and procedures.

11. POLICY AWARENESS AND UPDATE

11.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Organisation's induction program, in the case of employees of the Organisation. Further training and additional awareness regarding the Policy will be offered from time to time by the Organisation. The Organisation will specifically make Users who are not employees of the Organisation aware of the Policy.

11.2. **Dissemination**: This Policy will be made available on the Organisation's network, intranet or similar portals.

11.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.