M3 INVESTMENT GROUP

PRIVACY POLICY

M3 Investment Group Pty Limited ACN 610 101 598: CAR 1239571 AFSL 456663

Our Commitment to Privacy

M3 Investment Group Pty Limited ACN 610 101 598 (M3, Us or We) is committed to protecting and securing the privacy and confidentiality of our client's personal information. We have developed our own privacy principles, which embody the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Privacy Act) (amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012). For the purposes of General Data Protection regulation (GDPR) this policy also explains how we process 'personal data'. We also comply with the Spam Act 2003, which deals with restrictions on sending emails. We do not and will never spam you!

1. Introduction

The Privacy Act requires that we handle your personal information in accordance with a set of national principles, known as the APPs, which regulate the collection, use, correction, disclosure and transfer of personal information about individuals by organisations like us in the private sector. We are required under various legislation and codes of practice to collect certain information about you in order to provide our range of services. These include, but are not limited to, the Corporations Act, Financial Transactions Reports Act, Anti-Money Laundering and Counter Terrorism Financing Act, Income Tax Assessment Act as well as certain regulations issued by the Australian Securities and Investments Commission (ASIC). In addition, our ability to provide you with comprehensive and quality services is reliant on us obtaining certain information about you.

2. Collection of Information

If you are a client of M3, we will collect and hold your personal information for the purposes of: • providing advice, products and services to you;

- managing and administering your products and services;
- establish and manage your investments and accounts;
- process contributions, transfer monies or pay benefits;
- report the investment performance of your account;
- verifying your identity;
- letting you know about our other products and services; and
- managing our relationship with you.

We may request personal and sensitive information (as those terms are defined in the Privacy Act) from you, which will generally comprise, but not be limited to, the following type of information: • personal details e.g. name, address, contact details (phone, email), date of birth, marital status, dependents, employment details; • trust or self-managed super fund details and beneficiaries; • business details, including ABNs; • details of all investments, superannuation, investor numbers, credit card and bank account details; • taxation information including your tax file number; and • details to qualify you as a "Wholesale" client as that term is defined in the Corporations Act 2001 (Cth).

If you do not provide us with the information required, we may elect to terminate our relationship with you, if we believe it will jeopardise our ability to provide you with a complete, accurate and comprehensive service. We will inform you of any legal requirements for us to ask for information about you and the consequences of not giving us that requested information. For example, in addition to the personal information we will obtain from you, whenever you acquire a new product or service from us, we will require documents evidencing your identity. Such evidence may include a certified copy of your driver's licence, passport or birth certificate.

We will only solicit personal information about you where you have knowingly provided that information to us, we believe you have authorised a third party to provide that information to us, or we are obligated by law to obtain such information. Third parties that we may need to collect information from include your financial adviser, product issuer, employer, accountant or solicitor. To verify your identity for Know Your Customer (KYC) purposes, we may also solicit personal information about you from reliable identity verification service providers.

3. Disclosure of Information

In certain instances, we may be required to provide your information to external parties. Prior to disclosing any of your personal information to another person or organisation, we will take all reasonable steps to satisfy ourselves that: a) the person or organisation has a commitment to protecting your personal information at least equal to our commitment, or b) you have consented to us in making the disclosure. From time to time we are required to disclose information to other organisations to comply with the laws and regulations governing our provision of services. The organisations we may be required to disclose information include, but are not limited to: • financial institutions that hold accounts for you (including fund managers, financial advisers, stock brokers); • organisations involved in providing, managing or administering our products or services such as actuaries, custodians, external dispute resolution services, insurers, investment managers, or mail houses; • to ASX Group, Chi-X Australia Pty Limited and The National Stock Exchange; • government departments e.g. The Office of the Australian Information Commissioner, Australian Taxation Office (ATO), ASIC and Centrelink as required by law; • external service providers and other compliance inspectors for audit purposes; • external parties for business acquisitions or in the event of the sale of the business; • any other external party which we are compelled at law to make disclosures to; and • any other external party as authorised by you from time to time. We will not use or disclose information collected about you other than for a purpose made known to you unless the disclosure is: • required by law (e.g. ATO, Australian Prudential Regulation Authority and ASIC have the power to order us to disclose information about your situation); • authorised by law (e.g. to protect our interests or where we have a duty to the public to disclose); • necessary to discharge obligations (such as to foreign governments for the purposes of foreign taxation) • you have consented to our disclosing the information to you, or; • the assets and operations of the business are transferred to another party. We undertake not to sell, rent or trade your personal information. We may use the personal information collected from you for the purpose of providing you with direct marketing material such as articles or research reports that may be of interest to you, however you may request not to receive such information by contacting M3 as set out below. Other than as set out in this document, we will not otherwise disclose your information to other parties without your explicit consent.

4. Disclosing your personal information overseas

We may use cloud storage to store the personal information we hold about you. We may store information about you in other types of networked or electronic storage. The cloud storage and the IT servers may be located outside Australia. It is generally unlikely that we will disclose your personal information overseas. However, any overseas disclosure does not affect our commitment to safeguarding your personal information and we will take reasonable steps to ensure any overseas recipient complies with the APPs. Where we may be transferring your personal information overseas, we will either seek your consent or inform you and ensure that

appropriate contractual measures are in place requiring the overseas entity to protect your personal information in accordance with our obligations under Australian privacy law.

5. Access and correction of information

You may request access to the personal information we hold about you. We may charge a reasonable fee to cover our costs. There may be circumstances where we are unable to give you access to the information that you have requested. If this is the case, we will inform you and explain the reasons why. We will take reasonable steps to ensure that the personal information we collect, hold, use or disclose is accurate, complete, up to date, relevant and not misleading. You have a right to ask us to correct any information we hold about you if you believe it is inaccurate, incomplete, out of date, irrelevant or is misleading. If we do not agree with the corrections you have supplied and refuse to correct the personal information, we are required to give you a written notice to that effect and a statement if requested. If you wish to access or correct your personal information, you may contact us through our offices or by writing to the Privacy Officer, whose contact details are set out in section 10.

6. Exercising your other rights

You have a number of other rights in relation to the personal data we hold about you. You have the right to: • seek human review of automated decision-making or profiling, such as you have the right to review the risk profile that has been generated based on your answers about your personal circumstances and tolerance to risk and to either agree or disagree with the result; • opt-out of direct marketing, and profiling for marketing; to opt out, simply choose 'unsubscribe' on the email or publication received; • opt-out of processing for research / statistical purposes, or processing on the grounds of 'pubic interest' or legitimate interest'; • erasure, you have the right to ask us to delete or remove your personal data where there is no legitimate reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing. Note, however that we may not always be able to comply with your request for erasure due to relevant retention periods and legal requirements; • data portability, upon your request we can provide you or a third party you have chosen with your personal information in a structured, commonly used, machine-readable format; and • temporary restriction or processing - you have the right to object or restrict us using your personal data. To seek to exercise any of these rights, please contact our Privacy Officer.

7. Security and Retention Policy

We are committed to ensuring the security of personal information that we hold about you. We take reasonable steps to ensure the personal information we hold about you is stored securely, whether in a physical or electronic form. Some of the ways we do this are: • confidentiality requirements of our employees, agents and authorised representatives; • use of document storage security services are subject to regular audit and the people who handle your personal information have the training, knowledge, skills and commitment to protect it from unauthorised access, disclosure or misuse; • security measures for access to our systems; • only giving access to personal information to a person who is verified to be able to receive that information; and • electronic security systems such as firewalls and data encryption. You should note that there are inherent security risks in transmitting information through the internet or by electronic mail (E-mail). We do not have control over the transfer of personal information over the internet and we cannot guarantee its security. You should assess these potential risks when deciding whether to use online services. If you do not wish to transmit information through our website or email, there are other ways in which you can provide this information to us. You can, for example, contact our Privacy Officer as set out in section 10. We are required by law to retain certain records of information for varying lengths of time and, in certain circumstances, permanently. Where your personal information is not required to be retained under law and is no longer required for the

purpose for which it was collected, we will take reasonable steps to irrevocably destroy or de-identify it.

8. Complaints and breaches

If you believe that we have breached the APPs by mishandling your information, you may lodge a written complaint addressed to the Privacy Officer, whose contact details are set out in this section 10. Our Privacy Officer will respond to your complaint within 30 days of its receipt. At all times we will seek to manage your complaint in accordance with following principles: • all complaints will be treated seriously; • all complaints will be dealt with promptly; • all complaints will be dealt with in a confidential manner; and • the privacy complaint will not affect your existing obligations or the commercial arrangements that exist between this us and you. In the event that the Privacy Officer is unable to resolve your complaint, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC). You can lodge a written complaint with the Australian Information Commissioner by: • post to GPO Box 5218, Sydney NSW 2001; • submitting an online or hard copy form which may be accessed through the Australian Information Commissioner's website at www.oaic.gov.au or obtained from https://forms.business.gov.au/aba/oaic/privacy-complaint-/; • fax to 02 9284 9666; or • email at enquiries@oaic.gov.au If you are in the European Union, you can choose to instead lodge a complaint with your local Data Protection Authority (DPA). The list of DPA's is at http://ec.europa.eu/justice/article-29/structure/dataprotection-authorities/index_en.htm. We are committed to helping you have control of your personal information and so it is our practice to take reasonable steps to notify you if we are aware that we have breached your privacy.

9. Notifiable Data Breach Scheme

We may be required to make mandatory disclosures of any data breach we experience in accordance with the Notifiable Data Breach Scheme (Australia) established by the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth). If we are required to make a mandatory disclosure under the data breach act and that data breach relates to your information, we will notify you of same as soon as practicable in the manner required by the Scheme and the Australian Information Commissioner.

10. Contacting the Privacy Officer

You can contact the Privacy Officer by post, email or telephone: Privacy Officer M3 Investment Group Pty Limited Level 25, Three International Towers, 300 Barangaroo Ave, Barangaroo, NSW 2000 emmanuel.yi@m3group.com.au 02 8277 4515. For the purposes of GDPR, M3 Privacy Officer is also our Data Protection Officer.

11. Consent

If you do not consent to the use or disclosure of your personal information in the manner indicated above or in our Privacy Policy as amended from time to time, contact our Privacy Officer using the details provided above. Please note that you can withdraw your consent, without any charge, by contacting us at any time.

12. Changes to this Privacy Policy

Please note that this Privacy Policy may change from time to time. You may at any time request a current copy from our Privacy Officer or access it from our website at www.brsa.com.au. We encourage you to review our Privacy Policy periodically for any changes. This Privacy Policy came into existence on 1 August 2018.

13. Need more information?

If you have a query concerning how your personal information is collected and used or regarding M3 Privacy Policy, please contact our Privacy Officer at emmanuel.yi@m3group.com.au.

Additional information, including the Australian Privacy Principles, may be found on the OAIC website at www.oaic.gov.au.

14. General Data Protection Regulation 2016/679

If you are an individual resident of an EU member state, then the GDPR applies to our collection, storage and use of your information. In addition to the general provisions set out in this document, the provisions in this section will apply to you and to the extent of any conflict with the general provisions, the provisions in this section will prevail. 1. As we are incorporated in Australia, you acknowledge and expressly agree that all of your information will be transmitted outside of the EU and in particular to Australia for processing purposes. 2. We may be required to disclose your information to any governmental body, supervisory authority or regulator in the EU as required by the GDPR from time to time. We may also be required to make mandatory disclosures of any data breaches relating to your information in accordance with the GDPR. 3. If you request a copy of any information held about you, then to the extent reasonably possible (and provided the general provisions of this document relating to such a request are met) then in accordance with the GDPR we will endeavour to provide such information in a structured, commonly used, machine-readable and interoperable format that enables data portability. 4. Any right you have to access, erasure and portability of your information under the GDPR is restricted in the manner set out in Article 23 of the GDPR. 5. In relation to any direct marketing activities undertaken by us or third-party providers in accordance with this document, you are entitled to object to such direct marketing activities. 6. You are entitled to object to any profiling of you that is undertaken by us, or automatically by machines, as a result of the collection and processing of your information. 7. We will, where reasonably practicable, encrypt your information. However, you acknowledge and agree that it is unreasonable and inappropriate for us to use pseudonyms for data processing in our ordinary course of business and in the delivery of services to you.