PRIVACY POLICY

This is the Privacy Policy of iInvest Trading & Advisory Pty Ltd. In this Privacy Policy 'iInvest Trading & Advisory ', 'we', 'our' and 'us' mean iInvest Trading & Advisory Pty Ltd ("iInvest"). If you want more information about this Privacy Policy, or if you want to inquire about any of your personal information, or if you believe your personal information is inaccurate, incomplete or out-of-date, contact us immediately.

If you give us personal information about another person, you represent that you are authorised to do so and agree to inform that person who we are, that we will use and disclose that information for the relevant purposes set out below, and that they can access the information we hold about them.

Your personal information will be treated strictly in accordance with the Australian Privacy Principles in the *Privacy Act 1988* (Cth), the Privacy Amendment Act 2012, Notifiable Data Breaches Scheme and the OAIC (as complaints regulator).

PERSONAL INFORMATION

Whilst the Australian Privacy Principles came into effect on 12 March 2014, some of the principles apply to information collected both prior to, and after, that date. Consequently, for personal information held prior to that date, in accordance with those particular principles, we will:

- Take reasonable steps to protect it from misuse, loss or unauthorised access or disclosure;
- Take reasonable stapes to ensure that such information, if used, is accurate, compete and up to date;
- Provide you with access to the information if we still use it;
- Not use any government identifier to identify you, and
- Only transfer such information overseas with your consent or as authorised by the principles.

The remainder of this document is concerned with personal information collected on or after 12 March 2014, except insofar as this Privacy Policy further addresses the particular principles reflected in the five matters above.

THE INFORMATION WE COLLECT

We collect personal information that we believe is necessary to deliver our services or products or otherwise for our primary business functions and/or activities.

Ordinarily we only collect information about you when you provide it to us or it is provided to us with your authority.

We collect personal information by lawful and fair means and not in an unreasonably intrusive way. The types of personal information we collect generally include your name, address, telephone number, email address, financial information, other contact or identification details and, in some cases, information necessary to make or receive payments to or from you or necessary to effect transactions in financial products on your behalf.

We will collect personal information directly from you when you apply for a product or a service, deal with us over the telephone or in person, send us a letter or email, or visit our website. On occasions, we may collect personal information about you from third parties, for example, share registries, ASIC and identification service providers.

If you fail to provide the personal information we reasonably request, we may not be permitted under the law to provide services to you, you may not receive payments owing to you as efficiently as possible, or we may not be able to communicate with you.

Apart from the necessity to collect your information in order to provide a service to you or maintain our relationship with you, the purposes for which we would generally collect and use your personal information will include:

- complying with legislative and regulatory requirements;
- performing our administrative operations, including accounting, risk management, record keeping, archiving, systems development and testing and staff training;
- conducting market or customer satisfaction research;
- inviting you to other events that may interest you;
- developing and identifying products and services that may interest you; and
- telling you about other products and services we offer (unless you ask us not to).

PERSONAL INFORMATION ABOUT THIRD PARTIES

If at any time you supply us with personal information about another person, you should ensure that you are authorised to do so and you must agree to inform that person who we are, that we will use and disclose that personal information, and that they may gain access to it should we hold that information.

DISCLOSURE OF PERSONAL INFORMATION

You authorise us to disclose necessary information to related companies, affiliates and any agents or contractors who provide services to us in connection with the provision of products or services you have sought from us. These parties are prohibited from using your personal information except for the specific purpose for which we supply it to them.

Subject to what is permitted by law, the types of third parties we may disclose your personal information to include:

- our agents, contractors, insurers and external advisers we engage from time to time to carry out, or advise on, our functions and activities;

- any person or organisation who introduces you to us;
- Our third party providers of trade execution, settlement and clearing services for ASX (and Cboe) listed products. Currently, Morrison Securities Pty Ltd, Australian Investment Exchange Limited and Interactive Brokers Australia Pty Ltd;
- regulatory bodies, government agencies, law enforcement bodies and courts;
- licensed financial markets (ie ASX) for the purpose of, amongst other things, compliance and surveillance activities;
- other financial institutions, and
- any person to the extent necessary, in our view, in order to carry out the instructions you give to us.

In some cases, we may need to transfer your personal information outside Australia. For example, if you trade in securities listed on overseas exchanges, we may be required to provide your personal information to our overseas agents. If we believe that the overseas third party is not subject to, or has not agreed to comply with, privacy obligations equivalent to those which apply to us, we will seek your consent to transfer the information, except where the Australian Privacy Principles do not require us to do so.

PURPOSE AND USE OF PERSONAL INFORMATION

We have collected and may use your information to do one or more of the following:

- open an account for you
- maintain your account
- process transactions on your behalf
- enable us to assess any request from you for financial advice
- send research information to you
- respond to any specific requests you may contact us about
- help us to assess products that may suit your financial needs
- notify you of any products that may be of interest to you
- keep you informed on matters that may affect or be related to your investments
- update your personal files
- enable us to meet our obligations under certain laws
- to assist you in determining your investment objectives and providing you with investment advice and information on new opportunities to assist you in achieving these objectives
- to provide you with regular reviews and keep you informed on the performance of your investments
- any purpose for which the information was requested and any directly related purpose
- developing, improving and marketing our products and services.

OUR WEBSITE

Our compliance with the Australian Privacy Principles also extends to when you transact business via our website. Our website terms and conditions and any privacy notices are clearly posted on the website.

When you use a link from our website to the websites of third parties, those websites are not subject to our Privacy Policy. Those third parties are responsible for informing you of their own privacy policies.

User names and passwords are required to access those areas of our website that are restricted to clients. You are reminded that these user names and passwords are strictly for your personal use only. You are responsible for all acts that result from any use of your user name and password, whether authorised or not, or that result from your failure to maintain security. You must notify us immediately if you consider that the security of your user name and password has been breached.

For statistical purposes we may collect information on website activity (such as the number of users who visit the website, their country, the date and time of visits, the number of pages viewed, navigation patterns and the operating systems and browsers used to access the site). This information on its own does not identify an individual but it does provide us with statistics that we can use to analyse and improve our website.

We also use cookies and measurement tools on our website, as do third parties such as analytics, who may monitor unidentifiable statistics relating to website access and usage. We use and disclose the unidentifiable information collected through the use of cookies and measurement tools in accordance with this Privacy Policy. This includes using the information to report statistics, analyse trends, diagnose problems and improve the quality of our products and services.

We may combine our cookies and information (collected through the cookies and measurement tools) on this website with other information (including information collected by third parties using their own cookies and measurement tools) to provide better or more relevant services and information.

If an individual does not want information collected through the use of cookies and/or measurement tools, they may be able to delete or reject cookies and/or some of
the measurement software features through their browser or the settings section of their mobile or tablet device. Disabling these features may cause some of the functions on the websites to work less effectively.

We provide links to external websites, as well as to third party websites that allow interaction and sharing of content including social media buttons such as Facebook share, Twitter, Pinterest, Instagram and Google+. These linked sites, applications and widgets are not under our control and we do not accept responsibility for the conduct of companies linked to our websites, or their collection of information through these third party applications or widgets. Before disclosing information on any other website, or using these applications or widgets users are advised to examine the terms and conditions of using that website and the relevant third party's data collection practices and privacy policy.

The Internet is not always a secure method of transmitting information. While iInvest takes reasonable steps to ensure all information it receives is maintained securely, it cannot ensure that communications conducted via the Internet will be secure.

ACCESSING YOUR PERSONAL INFORMATION

If at any time you wish to know what personal information we are holding about you, you are welcome to ask us for your details by writing to us in a form or manner which identifies the nature of the personal information requested. The appropriate contact is:

The Privacy Officer
iInvest Trading & Advisory Pty Ltd
11 West Street
BURLEIGH HEADS QLD 4220

Under certain circumstances we may not be able to tell you what personal information we hold about you. This includes where the information:

- relates to suspicions of unlawful activity, or misconduct of a serious nature and giving access would be likely to prejudice the taking of appropriate action in relation to the matter by iInvest Trading & Advisory or an enforcement body;
- would have an unreasonable impact on the privacy of another individual;
- relates to existing or anticipated legal proceedings with you;
- would reveal a commercially sensitive decision-making process or evaluative information; or
- prevents us by law from disclosing the information, or providing access which would prejudice certain investigations.

We may charge you a fee for accessing your personal information.

We will take reasonable steps to ensure that your personal information is accurate, complete and up to date.
If at any time, you find that current personal information we hold about you is inaccurate, incomplete or out of date, please contact us immediately and we will correct it, or advise you of any additional information we require to make the change.

SECURITY OF YOUR PERSONAL INFORMATION

We will take reasonable steps to protect the personal information we hold from misuse and loss, and from unauthorised access, modification or disclosure. In line with our internal authorisation and access policies, employees only have access to information on a need to know basis.

We take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.

However, no data transmission over the internet can be guaranteed as fully secure and we cannot guarantee or warrant the security of any information you send to us over the internet. You submit information over the internet at your own risk.

MARKETING

We may use your personal details, including your address and/or email address, to provide you with newsletters and information about products, services or other events that may be of interest to you.

If at any time you do not wish to receive such marketing information, you have the option to ask us not to send you any further such material – you may do so by emailing, phoning or writing to us.

COMPLAINTS

If you believe that the privacy of your personal information is not being adequately protected, you should contact our Privacy Officer. We will make every effort to resolve your complaint internally.

If we do not resolve your complaint to your satisfaction, you may apply to the Australian Information Commissioner to have your complaint investigated. For more information about how you may lodge a complaint with the Australian Information Commissioner, please contact the Commissioner's hotline service on 1300 363 992.

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.iinvestadvisory.com. We encourage you to review our Privacy Policy periodically for any changes.

ADDITIONAL INFORMATION

Additional information, including the Australian Privacy Principles, may be found the Australian Information Commissioner's website at www.oaic.gov.au.

DECLINING TO PROVIDE YOUR PERSONAL INFORMATION

If you do not give us your personal information, we may not be able to provide products and services as requested by you.

TELEPHONE RECORDING

We may record telephone conversations between you and persons working for iInvest. Such recordings or transcripts for such recordings may be used to resolve any dispute between you and iInvest.

CONTACT DETAILS

If you have any questions or would like further information regarding our Privacy Policy or our information handling practices, please contact us by:

E-mail: info@iinvestadvisory.com.au

Telephone: (07) 5520 8788

By Mail:
The Privacy Officer
iInvest Trading & Advisory Pty Ltd
11 West Street

BURLEIGH HEADS QLD 4220

Should you wish to obtain further information about privacy you can do so by visiting the Privacy Commissioner's website at www.privacy.gov.au

Appendix A

Data Breach Notification Procedure

1. Introduction

The Notifiable Data Breach reporting laws require all businesses caught by the Privacy Act 1988 to have a 'Data Breach Reporting' procedure in place.

2. What is a Data Breach?

A data breach is an unauthorised access or disclosure of personal information, or loss of personal information. Data breaches can have serious consequences, so it is important that we have robust systems and procedures in place to identify and respond effectively.

A data breach may be caused by malicious action (externally or internally), human error, or a failure in information handling or security systems. Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

3. Consequences of a data breach

Data breaches can cause significant harm in multiple ways. Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well being, financial loss, or damage to their reputation.

Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

A data breach can also negatively impact Authorised Representatives reputation for privacy protection, and as a result undercut our commercial interests. Authorised Representatives can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in our data breach response/s. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm and demonstrates that Authorised Representatives take their responsibility to protect personal information seriously.

4. Notification Data Breach (NDB) Requirements

Authorised Representative of Zodiac Securities Pty Ltd are required to notify affected individuals and the Office of the Australian Information Commissioner **(*OAIC*)** of eligible data breaches. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by Authorised Representatives (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- Authorised Representatives have been unable to prevent the likely risk of serious harm with remedial action.

If a suspected data breach occurs, Zodiac, iInvest or Fairway staff must immediately escalate the breach to the Managing Director ("MD") who will conduct an assessment to determine whether the breach is an 'eligible data breach' that triggers notification obligations.

Individuals must be notified if their personal information is involved in a data breach that is likely to result in serious harm. Once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

5. Data Breach Response Plan and Process

As data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities, there is no single way of responding to a data breach. Although each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks, the actions representatives will take following a data breach are:

1. The MD will contain the suspected or known data breach by taking immediate steps to limit any further access or distribution of the affected personal information or prevent any further compromise of other information.

2. The MD will consider whether the data breach is likely to result in serious harm to any of the individuals whose information was compromised. If there are "reasonable grounds" to believe this is the case, then notification is required. If there are only suspected grounds for this to be the case, then the MD will assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm. This assessment must be conducted within 30 days of the data breach.

3. Based on the documented assessment the MD will make an evidence-based decision about whether serious harm is likely. If it is determined that an eligible data breach has occurred, the MD will notify the impacted individuals and the OAIC by submitting the online form OAIC website. The MD will also consider if other relevant bodies should also be notified, i.e. ASIC, Police, Austrac, ATO etc.

4. The MD will review the incident and consider what actions can be taken to prevent future breaches.

5. The MD will maintain a Data Breach Register of any data breaches and notify the Board at least quarterly, including details of the reviews undertaken and remediation actions.

In addition at least annually, the MD will review the Data Breach Response Plan and test it to ensure it is current and effective by ensuring staff know what actions they are expected to take.