Privacy policy

Aubrey Capital Management Limited ("**Aubrey**", "**we**", "**us**" or "**our**") is committed to protecting the privacy of individuals whose data it processes ("**you**" or "**your**").

1. IMPORTANT INFORMATION AND WHO WE ARE

Aubrey is committed to protecting the privacy of individuals whose data it processes ("**you**" or "**your**") as a processor of certain funds that it manages including Aubrey Global Emerging Markets Opportunities Funds, S&W Aubrey Capital Management Investment Fund, Fondaco Lux EU Conviction Equities and our private clients (the "**Funds**") and/or on its own behalf as a controller.

This privacy policy aims to give you information on how Aubrey collects and processes your personal data as:

(a) a processor on behalf of the Funds that it manages; and

(b) a controller through your use of this website, by applying for employment and/or to work with Aubrey, by sending us correspondence and/or providing us with products and/or services.

In addition, it outlines your data protection rights under the EU data protection regime introduced by the General Data Protection Regulation (Regulation 2016/679) (the "**GDPR**").

This website is not intended for children and we do not knowingly collect data relating to children.

Please contact Aubrey Capital Management Limited (registered number SC299239), 10 Coates Crescent, Edinburgh, EH3 7AL if you have any queries in relation to the processing of your personal data under this policy.

We have appointed a data protection manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the data protection manager Iain Hay at Iain.Hay@aubreycm.co.uk.

2. CATEGORIES OF DATA SUBJECTS

(A) INVESTORS

The following section of this policy sets out how Aubrey, as processor of the Funds that it manages, will process personal data.

The kind of information we hold about you

We may hold personal data about investors in a Fund which is provided to us by you directly as a result of your holding and/or investment in the Funds (by completing application forms, through our website, telephone calls and/or corresponding with us) or which is provided to us by third parties including name, date of birth, national insurance number, email address, telephone numbers, copies of ID (including passport, drivers licence, bank or utility statements or council tax statements), bank account details, financial information and history, employment details and information on tax, PEP and details of dependents.

In connection with your holding and/or investment in the Funds, we may collect, store, and use the above categories of personal information about you.

How we will use information about you

Your personal data may be processed by Aubrey or its sub-processors (or any of their affiliates, agents, employees, delegates or sub-contractors) for the following purposes:

(a) to provide you with information on the Funds (including performance updates), which is being carried out to pursue Aubrey and/or the Funds' legitimate interests;

(b) to allow us to administer and manage your holding in the Funds (including fee calculations and the payment of dividends) which are necessary for the Funds to comply with applicable laws and/or in its legitimate interest;

(c) to update and maintain records for the Funds including with regulators and relevant company registers;

(d) to carry out anti-money laundering checks and other actions in an attempt to detect, prevent, investigate and prosecute fraud and crime, which Aubrey considers necessary for compliance with the Funds' legal obligations, for the performance of a task being carried out in the public interest and/ or to pursue the Funds' legitimate interests (including for the prevention of fraud, money laundering, sanctions, terrorist financing, bribery, corruption and tax evasion);

(e) to prepare tax related information in order to report to tax authorities in compliance with a legal obligation to which the Funds are subject; and

(f) to scan and monitor emails sent to us (including attachments) for viruses or malicious software, to process and encrypt personal data to protect and manage email traffic, and to store personal data on our systems to pursue our legitimate interests including for document retention purposes; and

(g) such other actions as are necessary to manage the activities and/or to comply with the legal obligations of the Funds, including by processing instructions, monitoring and recording electronic communications (including telephone calls and emails) for quality control, analysis and training purposes and enforcing or defending the rights and/or interests of the Funds, in order to comply with the Funds' legal obligations and/or to pursue the Funds' legitimate interests.

Basis on which we process your data

Where such processing is being carried out on the basis that it is necessary to pursue Aubrey and/or the Funds' legitimate interests, such legitimate interests are not overridden by your interests, fundamental rights or freedoms. Such processing may include the use of your personal data for the purposes of sending you electronic marketing communication, in relation to which you can at any time subscribe by following the instructions contained in each marketing communication.

Aubrey and/or the Funds do not anticipate being required to obtain your consent for the processing of your personal data as listed above. If Aubrey and/or the Funds wish to use your personal data for other purposes which do require your consent, Aubrey will contact you to request this.

(B) JOB APPLICANTS

The following section of this policy sets out how Aubrey may process personal data (as a controller) about applicants of jobs or placements and potential workers and contractors.

Aubrey is the data controller of the personal data that you provide, or which is provided to, or collected by Aubrey during and/or in connection with any application for a position at Aubrey.

The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of personal data about you: name, address and post code, telephone number, personal email address, emergency contact names and numbers, date of birth, gender, tax code, NI or SS number, bank account details, proof of ID (includes copies of passport photo page and utility bills), employment history, qualifications and other information contained in your CV and cover letter or email, details of referees and references, qualifications (including copy certificates of academic and professional qualifications), and information provided to us during telephone calls, interviews and/or meetings with you.

We may also collect, store and use the following "special categories" of sensitive personal data: information about your health, including any medical condition, health and sickness records and/or information about criminal convictions and offences.

We may collect personal data about candidates from the following sources: you, the candidate directly; recruitment agencies; background check providers; credit reference agencies; disclosure and barring service in respect of criminal convictions; your named referees; and data from third parties is from a publicly accessible source including Companies House records and social media (such as LinkedIn).

How we will use information about you

Your personal data may be processed by Aubrey or its sub-processors (or any of their affiliates, agents, employees, delegates or sub-contractors) for the following purposes:

- to assess your skills and qualifications, to consider your suitability for the position and to decide whether to enter into a contract with you;
- to carry out background and reference checks, where applicable;
- to communicate with you about and in connection with the recruitment process;
- to keep records related to our hiring processes;
- to comply with legal or regulatory requirements;
- to scan and monitor emails sent to us (including attachments) for viruses or malicious software, to process and encrypt personal data to protect and manage email traffic, and to store personal data on our systems to pursue our legitimate interests including for document retention purposes; and

- such other actions as are necessary to manage the activities of the Aubrey, including by processing instructions, monitoring and recording electronic communications (including telephone calls and emails) for quality control, analysis and training purposes and enforcing or defending the rights and interests of Aubrey, in order to comply with its legal obligations and/or to pursue its legitimate interests.

Basis on which we process your data

We process this personal data on the basis of our legitimate interests (in order to decide whether to appoint you to work for us) and/or in order to comply with applicable laws.

Once we receive your CV and covering letter or your application form, we may process that information to decide whether Aubrey has any suitable vacancies and if you meet the basic requirements to be shortlisted for that role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the work. If we decide to offer you the work, we will then take up references and we may carry out a criminal record or other checks before confirming your appointment.

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

We will use your sensitive personal data in the following ways:

- we will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during the interview; and

- we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure equal opportunity monitoring and reporting.

We may collect information about your criminal convictions history if we would like to offer you the work or a position (conditional on checks and any other conditions, such as references, being satisfactory). We are required to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- We are legally required by the Financial Conduct Authority (FCA) and the Securities and Exchange Commission (SEC) to carry out criminal record checks for those carrying out controlled functions and / or involved in the administration of Fund cash or assets.

- The role requires a high degree of trust and integrity and so we would like to ask you to seek a basic disclosure of your criminal records history.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

We may share your personal data with the following third parties for the purposes of processing your application: employee screening and IT service providers.

If your application is successful, the information you provide during the application process will be retained by Aubrey as part of your employee file and held in accordance with our data retention policy or applicable laws.

If your application is unsuccessful, the information you have provided will be retained by Aubrey for six (6) months after we have communicated our decision to you. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations. If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

(C) VISITORS TO OUR WEBSITE

The following section of this policy sets out how Aubrey may process personal data (as a controller) about visitors to its website.

The kind of information we hold about you

We may collect, use, store and transfer different kinds of personal data about you which you provide to us though our website: technical data (including internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website, usage data (including information about how you use our website).

We do not collect any sensitive personal data or special categories of personal data about you through our website (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

How we collect your data

We use different methods to collect data from and about you including:

- direct interactions with you, including by filling in forms. This includes personal data you provide when you subscribe to our publications and/or request marketing to be sent to you.
- Automated technologies or interactions. As you interact with our website, we may automatically collect technical data about your equipment, browsing actions and patterns. We collect this personal

data by using cookies, server logs and other similar technologies. We may also receive technical data about you if you visit other websites employing our cookies.

How we will use information about you

Your personal data may be processed by Aubrey or its sub-processors (or any of their affiliates, agents, employees, delegates or sub-contractors) for the following purposes:

- to send you updates on the performance of the Funds, newsletters, invitations to events and other electronic marketing communications which we will do (a) on the basis of our legitimate interests if you are an investor in the Fund or (b) with your consent;
- to use data analytics to improve our website, marketing, customer experiences on the basis of our legitimate interests;
- to comply with legal or regulatory requirements;
- to scan and monitor emails sent to us (including attachments) for viruses or malicious software, to process and encrypt personal data to protect and manage email traffic, and to store personal data on our systems to pursue our legitimate interests including for document retention purposes; and
- such other actions as are necessary to manage the activities of Aubrey and/or the Funds, including by processing instructions, monitoring and recording electronic communications (including telephone calls and emails) for quality control, analysis and training purposes and enforcing or defending the rights and/or interests of Aubrey and/or the Funds, in order to comply with their legal and/or regulatory obligations and/or to pursue their legitimate interests.

We will use your personal data in the following circumstances: where it is necessary for our legitimate interests, or those of a third party (including in relation to the sending of electronic marketing communications) and where your interests and fundamental rights are not overridden by those interests, or where we need to comply with a legal or regulatory obligation.

Links to websites

Where the Website provides links to other websites, Aubrey is not responsible for the data protection/privacy/cookie usage policies of such other websites, and you should check these policies on such other websites if you have any concerns about them. If you use one of these links to leave our website, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting a linked website and such websites are not governed by this policy. You should always exercise caution and review the privacy policy applicable to the website in question.

Cookies: A cookie is a small file which asks permission to be placed on your computer. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular website. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

Overall, cookies help us provide a better website by enabling us to monitor which pages users find useful and which they don't. A cookie does not give us access to a user's computer or any information about them, other than the data they choose to share with us.

The browsers of most computers, smartphones and other web–enabled devices are usually set up to accept cookies. If your browser preferences allow it, you can configure your browser to accept all cookies, reject all cookies, or notify you when cookies are set. Each browser is different, so check the "Help" menu of your browser to learn about how to change your cookie preferences.

However, please remember that cookies are often used to enable and improve certain functions on our website. If you choose to switch certain cookies off, it will affect how our website works and you may not be able to access all or parts of our website.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

For more information on the cookies we use and the purposes for which we use them please refer to our Cookies Policy, available at www.aubreycm.co.uk

For further details on cookies (including how to turn them off) can be found at www.allaboutcookies.org.

(D) BUSINESS CONTACTS

The following section of this policy sets out how Aubrey may process personal data (as a controller) about its business contacts and (current, previous and/or potential) service providers (and employees of service providers) and data subjects that have provided a business card to, or have corresponded with, an employee of Aubrey.

The kind of information we hold about you

We may collect, use, store and transfer different kinds of personal data about you which you provide to us including: name, date of birth, address, email address, telephone numbers, place of work and job title.

We do not collect any sensitive personal data or special categories of personal data about you through our website (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

How we will use information about you

We will use your personal data in the following circumstances: where it is necessary for our legitimate interests, or those of a third party, (including in relation to the sending of electronic marketing communications) and where your interests and fundamental rights are not overridden or where we need to comply with a legal or regulatory obligation.

Your personal data may be processed by Aubrey or its sub-processors (or any of their affiliates, agents, employees, delegates or sub-contractors) for the following purposes:

- to hold your personal data on our system and to contact you on the basis of the legitimate interests of Aubrey and/or the Funds (including in connection with using the services that you provide);
- in respect of suppliers, to allow us to process payments and orders in respect of any goods and services provided;
- to send you updates on the performance of the Funds, newsletters, invitations to events and other electronic marketing communications which we will do (a) on the basis of our legitimate interests if you are an investor in the Fund or (b) with your consent;
- to comply with legal or regulatory requirements;
- to scan and monitor emails sent to us (including attachments) for viruses or malicious software, to process and encrypt personal data to protect and manage email traffic, and to store personal data on our systems to pursue our legitimate interests including for document retention purposes; and
- such other actions as are necessary to manage the activities of Aubrey and/or the Funds, including by processing instructions, monitoring and recording electronic communications (including telephone calls and emails) for quality control, analysis and training purposes] and enforcing or defending the rights or interests of Aubrey and/or the Funds, in order to comply with their legal obligations and/or to pursue their legitimate interests.

Basis on which we process your data and right to withdraw consent

If we consider it necessary to obtain your consent in relation to the use of your personal data (such as for sending emails to individuals that have not invested in the Funds), we will contact you to request this consent. In such circumstances, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. If you decide to provide your consent, you have the right to withdraw your consent at any time, although that will not affect the lawfulness of processes based on consent before its withdrawal. To withdraw your consent or to opt out of receiving marketing communication, please contact us at clientservices@aubreycm.co.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Where such processing is being carried out on the basis that it is necessary to pursue Aubrey and/or the Funds' legitimate interests, such legitimate interests do not override your interests, fundamental rights or freedoms. Such processing may include the use of your personal data for the purposes of sending you electronic marketing communication, in relation to which you can at any time subscribe by following the instructions contained in each marketing communication.

3. DISCLOSURES OF YOUR PERSONAL DATA

We will not disclose personal information we hold about you to any third party except as set out below.

We may disclose your personal data to other members of our group, to the Boards of the Funds, to third parties who are providing services to us and/or the Funds, including IT service providers, event management, PR and marketing service providers, background and/or credit reference services, processors of the Funds (including printers, registrars, company secretarial services, administrators) telephone service providers, document storage providers, backup and disaster recovery service providers**.**

We may also disclose personal data we hold to third parties:

(a) in the event that we sell any business or assets, in which case we may disclose personal data we hold about you to the prospective and actual buyer of such business or assets; and/or

(b) if we are permitted by law to disclose your personal data to that third party or are under a legal obligation to disclose your personal data to that third party.

4. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Details of retention periods for different aspects of your personal data are available in our retention policy which you can request from us by contacting us at Aubrey Capital Management Limited, 10 Coates Crescent, Edinburgh, EH3 7AL.

5. INTERNATIONAL TRANSFERS

We do not transfer your personal data outside the European Economic Area (EEA).

6. DATA SECURITY

Aubrey has put in place measures to ensure the security of the personal data it collects and stores about you. It will use its reasonable endeavours to protect your personal data from unauthorised disclosure and/or access, including through the use of network and database security measures, but it cannot guarantee the security of any data it collects and stores.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

7. YOUR LEGAL RIGHTS

In certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. This request will be responded to within 30 working days and you will be provided with a copy of the information we hold about you. If we require more time to respond fully to any request, we will notify you in writing within the 30-day period referred to. Any additional copies of any information we provide to you may be subject to a reasonable fee.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. We try to ensure that the information we hold about you is accurate and kept up-to-date by contacting you at regular intervals. However, if in the meantime you believe that any information we are holding about you is inaccurate, out-of-date or incomplete, please notify us at clientservices@aubreycm.co.uk as soon as possible. We will promptly correct or delete any information found to be incorrect.

- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- Request the transfer of your personal information to another party.

- Withdraw your consent. If we are processing your personal data on the basis of your consent, you have the right to withdraw such consent at any time. Withdrawing your consent will not affect the lawfulness of processes based on consent before its withdrawal. To withdraw your consent or to opt out of receiving marketing communication, please contact us at clientservices@aubreycm.co.uk or following the unsubscribe instructions included in each electronic marketing communication. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

If you wish to exercise any of the rights set out above, please contact clientservices@aubreycm.co.uk.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

8. CHANGES TO THIS PRIVACY NOTICE

We may update this privacy notice from time to time and will communicate such updates through our website. We may also notify you from time to time about the processing of your data.

9. FURTHER INFORMATION

If you have any queries about this policy or your personal data, or you wish to submit an access request or raise a complaint about the way your personal data has been handled, please do so in writing and address this to the Data Protection Manager at Aubrey Capital Management Limited, 10 Coates Crescent, Edinburgh, EH3 7AL or by email to iain.hay@aubreycm.co.uk.

Aubrey Capital Management Limited is a private limited company registered in Scotland (registered number SC299239) and its registered office address is 10 Coates Crescent, Edinburgh, EH3 7AL.

Data Protection and Privacy Policy

Approved by the Risk and Compliance Committee – 14th February 2023

PRIVACY POLICY AND CYBERSECURITY

U.S. Clients

A. REGULATION S-P

Aubrey has implemented the below Privacy Policy in order to safeguard the personal information of its *consumers* and *customers* who advisory clients in accordance with the Gramm-Leach-Bliley Act of 1999 and its implementing regulations as promulgated by the Securities and Exchange Commission (17 CFR 248) ("Regulation S-P"), the Federal Trade Commission (16 CFR 313), and the Commodity Futures Trading Commission (17 CFR 160). As an investment adviser registered with the SEC, Aubrey is required to comply with the Gramm-Leach-Bliley Act of 1999 with respect to both its U.S. and non-U.S. Clients. For this Privacy Policy's purposes, the term "implementing regulations" shall refer to 17 CFR 248, 16 CFR 313, and 17 CFR 160. All questions regarding this policy should be directed to the Chief Compliance Officer. The Privacy Policy may be amended only by action of the Company's executive officers.

(1) Definitions for purposes of this Privacy Policy:

(a) *Consumer*. The term "consumer" has the meaning set forth in the Gramm-Leach-Bliley Act of 1999 and its implementing regulations. A consumer of the Company is deemed to include any individual, or its legal representative, who obtains or has obtained a financial product or service from the Company that is to be used primarily for personal, family or household purposes. An individual is deemed a consumer of the Company if he or she provides nonpublic personal information to the Company in connection with a potential investment with the Company, whether or not such individual enters into an advisory agreement with the Company. An individual is not the Company's consumer, however, if he or she provides the Company only with his or her name, address, and general areas of investment interest in connection with a request for information.

(b) *Consumer Report*. The term "Consumer Report" shall mean any written, oral, or other communication of any information by a consumer reporting agency bearing on a Consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under Section 604 of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(1)).

(c) *Consumer Report Information*. The term "Consumer Report Information" shall mean any record about an individual, whether in paper, electronic or other form that is a Consumer Report or is derived from a Consumer Report. Consumer Report Information also means a compilation of such records. Consumer Report Information does not include information that does not identify individuals, such as aggregate information or blind data.

(d) *Customer*. The term "customer" has the meaning set forth in the Gramm-Leach-Bliley Act of 1999 and its implementing regulations. A customer is deemed to include any consumer who has an account

managed by the Company. For this Company's purposes, the term "customer" includes advisory clients of Aubrey.

(e) *Disposal.* The term "Disposal" shall mean (i) the discarding or abandonment of Consumer Report Information; or (ii) the sale, donation, or transfer of any medium, including computer equipment on which computer information is stored.

(f) *Nonpublic Personal Information*. The term "nonpublic personal information" has the meaning as that set forth in the Gramm-Leach-Bliley Act of 1999 and its implementing regulations. Such information is deemed to include personally identifiable financial information that the Company has obtained from, been provided by or results from a financial product or services transaction with, customers and consumers that is not publicly available. Nonpublic personal information is deemed to include, among other things, (i) customer application information, information concerning customer transactions and accounts, and information collected from "cookies" through websites operated by the Company, (ii) any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using personally identifiable financial information that is not publicly available, and (iii) any publicly available information of a consumer that is described in a manner that indicates that the individual is a consumer of the Company.

This Company collects the following types of nonpublic personal information from Clients: name, address, social security number/tax identification number, telephone number, email address, date of birth, net worth.

(2) Commitment: The Company is committed to protecting the confidentiality and security of consumer, customer and former customer information the Company collects and will disclose such information only in accordance with the Gramm-Leach-Bliley Act of 1999 and its implementing regulations, any other applicable law, rules and regulations and this Privacy Policy.

(3) Scope: This Privacy Policy applies to the Company. The Company conducts its business affairs primarily through their employees. To the extent that service providers are utilized in servicing accounts the appropriate confidentiality agreements will be put into place.

(4) Procedures to Safeguard Consumer and Customer Records and Information Policies: The Company shall (a) insure the security and confidentiality of consumer, customer and former customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of consumer, customer and former customer records and information; and (c) protect against unauthorized access to or use of consumer or customer records or information that could result in substantial harm or inconvenience to any customer. Therefore, the Company has adopted the following policies:

(A) *Restricting Access to Those Who Need to Know.* To restrict access to nonpublic personal information about consumers, customers and former customers to those who need to know that information to provide products and services to such consumers and customers.

(B) *Safeguards.* To maintain physical, electronic, and procedural safeguards that comply with federal standards to guard nonpublic personal information about consumers, customers and former customers. See also "Cybersecurity" below.

(C) *Affiliate Disclosure.* To share nonpublic personal information of consumers, customers and former customers with its affiliates, subject to the consumers or customers expressly prohibiting such sharing.

(D) *Nonaffiliate Disclosure.* Not to share nonpublic personal information of consumers, customers and former customers with nonaffiliated third parties other than (i) to non-affiliated third parties involved in the account's everyday business purposes including but not limited to processing transactions, maintaining accounts, responding to court orders and legal investigations and/or reporting to credit bureaus, (ii) as permitted[1] or required by law and/or (iii) unless otherwise authorized to do so by the consumer or customer.

The Company will direct each nonaffiliated third party service provider (the "service provider") to adhere to this Privacy Policy with respect to all consumer, customer and former customer information of the Company and to take all actions reasonably necessary so that the Company is in compliance with this Privacy Policy.

(E) *Disposal.* To properly dispose of Consumer Report Information that it is not legally bound to maintain and wishes to dispose of, and shall take reasonable measures to protect against unauthorized access to or use of the Consumer Report Information in connection with the disposal of such information.

(F) *Privacy Notices.* To deliver initial and annual privacy policy notices in accordance with the Gramm-Leach-Bliley Act of 1999 and its implementing regulations.

Initial notices shall be distributed to all current customers of the Company as soon as possible after the adoption of this Privacy Policy. Thereafter, initial notices shall be delivered to each new customer upon the establishment of a customer relationship, as that term is defined in the Gramm-Leach-Bliley Act of 1999 and its implementing regulations, which, for the purposes of this Privacy Policy, shall be deemed to occur upon the inception of an account managed by the Company and/or its Affiliates.

The annual privacy policy notice will be sent at least every twelve (12) months in compliance with the Gramm-Leach-Bliley Act of 1999 and its implementing regulations.

[1] The exceptions for the sharing of nonpublic personal information pursuant to paragraph 4(D) above are presently contemplated to be only those allowed by Rules 14 and 15 of the implementing regulations. See Exceptions Pursuant to Rules 14 and 15 of the Gramm-Leach-Bliley Act of 1999 and Its Implementing Regulations" in item 14 below.

Amended privacy policy notices shall be distributed to all current customers of the Company as soon as possible after the adoption of the amended Privacy Policy. The amended privacy policy notice shall be delivered in accordance with the Gramm-Leach-Bliley Act and its implementing regulations.

(G) *Evaluation of Procedures*. The Chief Compliance Officer shall periodically evaluate the Company's procedures to ensure compliance with this Privacy Policy. In evaluating these procedures, the Chief Compliance Officer shall consider all or certain of the items listed on the Information Security Checklist set forth below. The items of the Information Security Checklist are not mandatory but shall be used by the Chief Compliance Officer as a guide to ensure the Company has implemented such procedures, as the Chief Compliance Officer, in consultation with the Company's executive officers, deems appropriate, to comply with this Privacy Policy.

The following is a non-binding, non-exclusive checklist of items to consider in the review of the Company's and its affiliates' internal policies and procedures.

(i) access rights to customer information;

(ii) access controls on customer information systems, including controls to authenticate and grant access only to authorized employees, individuals, and companies;

(iii) access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

(iv) encryption of electronic customer information;

(v) monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

(vi) response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected (see below "Responding to Privacy Breaches");

(vii) safekeeping of obtained materials containing nonpublic personal information in a secure location and restricting access to such materials to authorized employees, individuals, and companies; and

(viii) periodic review of the Company's information security program.

(6) Responding to Privacy Breaches: All employees must report to the Chief Compliance Officer any known or suspected breaches of the Company's privacy policy. The Chief Compliance Officer shall then report to the Company's Chief Operating Officer any material breach of this Privacy Policy that the Chief Compliance Officer has become aware of, or has received notice of from third party service providers. Upon being informed of any such breach, the Company's executive officers are authorized to take any such action they

deem necessary or appropriate to enforce this Privacy Policy and otherwise comply with the Gramm-Leach-Bliley Act of 1999 and its implementing regulations, including (i) taking any actions necessary to prevent further improper disclosures, (ii) informing counsel or appropriate regulatory authorities, (iii) notifying Clients as determined by the Chief Compliance Officer and (iv) revising these privacy policies. The Company shall document responsive actions taken in connection with any breach of security, and conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices.

(7) Exceptions Pursuant to Rules 14 and 15 of Gramm-Leach-Bliley Act of 1999 and Its Implementing Regulations.

In accordance with Rule 14 of the implementing regulations, the Company may disclose nonpublic personal information to its nonaffiliated third party service providers *as necessary to effect, administer, or enforce a transaction* that our customer requests or authorizes, or in connection with: (1) processing or servicing a financial product or service that a customer requests or authorizes; (2) maintaining or servicing the customer's account; or (3) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the customer.

Necessary to effect, administer, or enforce a transaction means that the disclosure is:

(1) required, or is one of the lawful or appropriate methods, to enforce the fund's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) is required or is a usual, appropriate, or acceptable method:

(a) to carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the customer's account in the ordinary course of providing the financial service or financial product;

(b) to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) to provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the customer or the customer's agent or broker;

(d) to accrue or recognize incentives or bonuses associated with the transaction that are provided by the Company or any other party;

(e) to underwrite insurance at the customer's request or for reinsurance purposes, or for any of the following purposes as they relate to a customer's insurance account administration, reporting, investigating, or preventing fraud or material

misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by federal or state law; or

(f) in connection with:

(i) the authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means;

(ii) the transfer of receivables, accounts, or interests therein; or

(iii) the audit of debit, credit, or other payment information.

In accordance with Rule 15 of the implementing regulations, the Company may disclose nonpublic personal information:

(1) with the consent or at the direction of the customer, provided that the customer has not revoked the consent or direction;

(2)

(a) To protect the confidentiality or security of the Company's records pertaining to the customer, service, product, or transaction;

(b) To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(c) For required institutional risk control or for resolving consumer and/or customer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the customer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the customer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a fund, persons that are assessing the Company's and its Affiliates' compliance with industry standards, and the Company's attorneys, accountants, and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including a federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, with respect to any person domiciled in that insurance authority's state that is engaged in providing insurance, and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(5)

(a) To a consumer reporting agency in accordance with the Fair Credit Reporting Act, or

(b) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely customers of such business or unit; or

(7)

(a) To comply with federal, state, or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by federal, state, or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over the Company and its affiliates for examination, compliance, or other purposes as authorized by law.

B. REGULATION S-AM ("REG S-AM")

Regulation S-AM prohibits certain entities, including registered investment advisers such as the Company, from using information about an individual consumer that has been obtained from an affiliated entity for marketing purposes unless (i) the potential marketing use of that information has been clearly, conspicuously and concisely disclosed to the consumer; (ii) the consumer has been provided a reasonable

opportunity and a simple method to opt out of receiving the marketing solicitations; and (iii) the consumer has not opted out.

C. REGULATION S-ID ("RED FLAGS RULES")

Under the Red Flag Rules, SEC and CFTC-regulated entities, including registered broker-dealers, investment companies and investment advisers, that meet the definition of "financial institution[2]" or "creditor[3]" and that offer or maintain a "covered account" are required to implement identity theft/red flags prevention programs that are designed to detect, prevent, and mitigate identity theft in cases with existing covered accounts or the opening of new covered accounts and are appropriate to the size and complexity of the Company as well as the nature and scope of the Company's activities.

The Red Flags Rules require each SEC and CFTC-regulated entity which is a financial institution or creditor to periodically assess whether it offers or maintains any covered accounts, in which case the Company would be required to implement identity theft prevention programs according to the parameters of the Red Flags Rules. "Covered accounts" are defined to include (i) an account that is primarily for personal, family or household purposes that is designed to permit multiple payments or transactions and (ii) any other account for which there is a reasonably foreseeable risk of identity theft to natural person customers or to the safety and soundness of the adviser.

Examples of arrangements that could cause the Company to be deemed a financial institution for purposes of the Red Flags Rules include: (i) the Company having the ability to direct transfers or payments from one or more natural persons' accounts to third parties, either unilaterally or upon the instructions of the natural person account owners; and (ii) the Company managing a private fund with one or more natural person investors that permit the Company or a related person to direct the natural person's redemption proceeds to third parties.

FIRST, the Company monitors the following to identify red flags:

i. Presentation of suspicious documents;

- E.g., documents provided for identification that appear to have been altered or forged.

[2] The term "financial institution" is defined to include any "person that, directly or indirectly, holds a transaction account belonging to a consumer." A "transaction account" includes any account that allows the account holder to make withdrawals by negotiable or transferable instrument, payment orders, telephonic transfers or similar transactions for the purpose of making payments or transfers to third persons. A "consumer" is defined to include natural persons.

[3] The term "creditor" is defined to include, among other things, persons who regularly extend, renew or continue credit as well as persons who regularly arrange for the extension, renewal or continuation of credit. A person would not be deemed to be a creditor solely because it bills for services in arrears, or because it advances funds for expenses incidental to the provision of a service. The SEC has stated that an investment adviser to a private fund that regularly and in the ordinary course of business lends money to permit individual investors to invest in the fund could qualify as a creditor.

ii. presentation of suspicious personal identifying information, such as a suspicious address change

iii. unusual use of, or other suspicious activity related to, a covered account

- E.g., (a) shortly following the notice of a change of address for a covered account, the Company receives a request for a new, additional, or replacement means of accessing the account or for the addition of an authorized user on the account; or (b) mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account); and

iv. notice from investors, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the Company

SECOND, the Company has the following policies to detect red flags:

i. The Company trains staff to the extent the Chief Compliance Officer determines necessary to effectively implement its identity theft program. As of the date hereof, the Chief Compliance Officer is responsible for implementing the program.

ii. to the extent any of the red flags detection, prevention and mitigation is outsourced by the Company (currently, it is not), it shall monitor such third party service provider.

iii. All employees are to notify the Chief Compliance Officer of any mail sent to investors if any of the red flags presented above are detected.

THIRD, if one or more red flags are detected, the Company shall respond in a matter commensurate with the degree of risk posed. Such appropriate responses may include, but are not limited to:

i. monitoring a covered account for evidence of identity theft;

ii. contacting the investor;

iii. changing any passwords or other security devices that permit access to a covered account;

iv. notifying law enforcement; or

v. determining that no response is warranted under the particular circumstances.

FINALLY, as part of its annual review of its Compliance Manual, the Chief Compliance Officer will review this program and update this policy (including red flags determined by the Chief Compliance Officer to be relevant)

to reflect changes in risks to investors and to the safety and soundness of the Company from identity theft based on factors such as:

i. the experiences of the Company with identity theft;

ii. changes in methods of identity theft;

iii. changes in methods to detect, prevent, and mitigate identity theft; and

iv. changes in the business arrangements of the Company (including mergers and service provider arrangements).

D. CYBERSECURITY

Because the internet is not a secure environment, the SEC has concerns surrounding the implementation of appropriate physical, electronic and procedural safeguards to protect the privacy of client and/or investor information and the interception of files and email containing such information. Accordingly, the Company has implemented certain procedures, safeguards and controls designed to prevent, detect and respond to a cyber-related threat, interception or other improper disclosure of investor confidential information as set forth below.

Policies:

(i) Employees cannot install or load onto any Aubrey computer any software, files or programs (including, but not limited to, any instant messaging program) purchased by the employee or downloaded or obtained from external sources without prior approval from the Chief Operating Officer.

(ii) Employees shall not use the communications equipment, including, but not limited to, Aubrey's telephones, facsimiles, voice mail, e-mail system and Internet access to knowingly send, receive, download, upload, access or review any material that contains worms, viruses, Trojan horses or other computer programming routines or engines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, date or information;

(iii) Employees should attempt to limit the amount of confidential, classified, or proprietary information that is transmitted electronically to only that which is necessary and required to conduct one's job.

(iv) As referenced in "Responding to Privacy Breaches" above, in the event confidential or proprietary information is lost, disclosed to or intercepted by unauthorized parties employees shall immediately notify the Chief Compliance Officer. In addition, the Chief Compliance Officer should be notified of any unauthorized use of Aubrey's information systems. Similarly, when passwords are (or are suspected of being) lost or stolen the Chief Compliance Officer should be notified immediately. All unusual system behavior, such as missing files, frequent

systems crashes, misrouted messages and the like should be reported immediately to the Chief Compliance Officer as one of these issues may indicate a computer virus infection or similar security problem.

(v) Employees must use passwords for access to Aubrey's computers.[4] Passwords shall be kept confidential and shall not be shared except as necessary to achieve such business purpose. Furthermore, passwords shall not be stored where unauthorized persons may discover them. Passwords shall be changed if there is reason to believe the password has been compromised and, in any event, changed periodically. All access and permissions for terminated employees shall be removed from the network system promptly upon notification of the termination.

To avoid unauthorized access, Employees must be mindful to close out programs and lock their terminals when they leave the office for an extended period of time.

(vi) As noted in the Company's Email Policy, employees must only conduct Aubrey related business on Aubrey servers and not any personal or third party servers.

(vii) External drives are not to be used to carry company documents unless the drives are equipped with built-in encryption. When using an approved Company laptop, no company documents are to be saved on the local hard drive (as such information will then not be encrypted).

Procedures and Safeguards:

(viii) The Company's servers are protected by an Enterprise-grade Sophos firewall which is provided by Technology Services Group (TSG) and is managed and monitored by their security specialists at their Support Centre. The servers are actively monitored for malware.

(ix) The Company has an incident response plan in the event of a cybersecurity breach.

(x) The Company has procedures in place for data backup and retrieval.

(xi) Servers are located at Aubrey Capital Management's Head Office

(xii) Access to the servers is accomplished by use of a Autotask Endpoint Manager

[4] It is still possible for others to access electronic documents and messages. Aubrey's use of such security features is designed to lessen the possibility of inadvertent or unauthorized access to such documents and messages both internally and externally. These security features are not in place to create or protect employee privacy.

(xiii) The Company routinely tests response plans and safeguards to evaluate the effectiveness of the cybersecurity policies and procedures, including:

a. The nature, sensitivity and location of information that the Company collects, processes and/or stores, and the technology systems it uses;

b. Internal and external cybersecurity threats to any vulnerabilities of the firm's information and technology systems;

c. Security controls and processes currently in place;

d. The impact should the information or technology systems become compromised and

e. The effectiveness of the governance structure for the management of cybersecurity risk.

Approved Aubrey Risk & Compliance Committee August 2025