Privacy Policy

We attach great importance to your privacy protection. When you use our platform to invest, we will inform you through the Privacy Protection Guide (hereinafter referred to as "this Guide") how we collect, use, store and share your personal information, as well as how you can access, update, control and protect your personal information, and explain your rights.

This Guide is closely related to your use of our services. We recommend that you read and understand the entire content of this Guide carefully and make the choices you think are appropriate. We strive to use concise and concise text to help you better understand the content of this Guide. If you agree to the content of this Privacy Policy (including updated versions), it means that you will agree that we will collect, use, save and share your relevant information in accordance with this Privacy Policy.

This Guide applies to PC, WEB, WAP and products whose software copyright belongs to Snowealth Company. We will strictly implement it in accordance with the requirements of national laws and regulations. When this Guide conflicts with laws and regulations, the latest laws and regulations shall prevail.

The main points of this Guide are as follows:

1. In order to facilitate your understanding of the types and uses of information we need to collect when you use our services, we will explain them to you one by one below.

2. In order to provide you with the services you need, we will collect your information in accordance with the principles of legality, legitimacy and necessity.

3. If your information needs to be shared with a third party in order to provide you with services, we will evaluate the legality, legitimacy and necessity of the third party's collection of information. We will require the third party to take protective measures for your information and strictly comply with relevant laws, regulations and regulatory requirements. In addition, we will obtain your consent or confirm that the third party has obtained your consent in the form of confirming the agreement, text confirmation in specific scenarios, pop-up prompts, etc. in accordance with the requirements of laws, regulations and national standards.

4. If your information needs to be obtained from a third party in order to provide you with services, we will require the third party to explain the source of the information and require the third party to

ensure the legality of the information it provides; if the personal information processing activities required for our business exceed the scope of your original authorization when providing personal information to a third party, we will obtain your explicit consent.

5. You can access and manage your information, cancel your pass account, securities account or make complaints and reports in the manner described in this guide.

We may obtain the account information (avatar, nickname) that you authorize to share from a third party, and bind your third-party account with the East Fortune Pass account after you agree to this privacy policy, so that you can directly log in and use our products and/or services through the third-party account. We will use your personal information in accordance with the agreement with the third party and after confirming the legitimacy of the source of personal information, and in compliance with relevant laws and regulations.

6. Protection

1) In order to protect your information security, we will take various reasonable and necessary measures to protect your information after collecting your information. For example, in the technical development environment, we only use de-identified information data. We will store

de-identified information separately from information that can be used to restore personal identification, to ensure that individuals are not re-identified in the subsequent processing of de-identified information.

2) To protect your information security, we are committed to using various security technologies and supporting management systems to minimize the risk of your information being leaked, damaged, misused, unauthorized access, unauthorized disclosure and altered. For example: encrypted transmission through network security layer software (SSL), encrypted information storage, and strict restrictions on access to data centers. When transmitting and storing personal sensitive information, we will adopt security measures such as encryption, permission control, and de-identification.