凱基金融控股股份有限公司
資訊安全宣告

凱基金融控股股份有限公司 (以下簡稱為本公司)秉持資訊安全理念，對於本公司資訊系統暨所儲存、處理、傳遞或揭露之資料作周全保護與防範，以杜絕毀損、失竊、洩漏、竄改、濫用與侵權等事件發生，特訂定本資訊安全聲明，相關資訊安全聲明如下：

一、本公司管理階層宣示支持資訊安全之決心，持續改善資訊安全管理系統以保護本公司資訊資產，降低資訊安全事故可能帶來之衝擊，以保障客戶之權益。

二、與本公司有業務往來之供應商及其員工與臨時雇員，應遵循合約、本公司「資訊安全管理政策」及相關資訊安全規範。存取合約範圍內之本公司資訊資產前應取得授權；持有或使用本公司之資訊資產時負保護之責任，防止遭未經授權之存取、竄改、破壞或不當揭露；中止或結束合約時應歸還本公司之資訊資產。

三、與本公司有業務往來之供應商及其員工與臨時雇員依照合約執行業務時，發現資訊安全事故或有違反本公司「資訊安全管理政策」或相關資訊安全規範之虞時，應立即通報本公司聯繫窗口。

四、所有資訊系統之開發、修改及維護，皆須符合相關資訊安全之規範並遵循本公司「資訊安全管理政策」之規定。

五、本公司所有人員在知悉發生資訊安全事故或違反「資訊安全管理政策」或規範之虞者，應依相關內部規章通報內外部單位，應變處理並分析根因預防再發生。

六、本公司遵循內外部相關法令規定，建立對應之管控程序，定期執行資訊安全查核作業，以確保資訊安全管理制度之持續有效運作。

此聲明之頒布，明確宣示本公司對於資訊安全的重視，與本公司有業務往來之廠商及其員工、臨時雇員應確實瞭解資訊安全聲明，以維護本公司資

訊安全。

KGI Financial Holding Co., Ltd.

Information Security Statement

KGI Financial Holding Co., Ltd. (the company) upholds the concept of information security, providing comprehensive protection for the company's information systems and the data stored, processed, transmitted, or disclosed. This is to prevent incidents such as damage, theft, leakage, alteration, misuse, and infringement. This Information Security Statement has been prepared in accordance with the following information security statements:

1. The management of the company declares its determination to support information security, continuously improving the information security management system to protect the company's information assets, reduce the impact of potential information security incidents, and safeguard the rights and interests of customers.

2. All suppliers, including their full-time and temporary employees, must comply with the contract, the company's "Information Security Management Policy," and related information security regulations. Authorization must be obtained before accessing the company's information assets within the scope of the contract; when holding or using the company's information assets, they are responsible for protecting them to prevent unauthorized access, alteration, destruction, or improper disclosure. Upon termination or closing of the contract, the company's information assets must be returned.

3. When suppliers, including their full-time and temporary employees, encounter information security incidents or potential violations of the company's "Information Security Management Policy" or related information security regulations during the execution of their contracted duties, they

should immediately report to the company's contact window.

4. All information system development, modification, and maintenance must comply with relevant information security regulations and adhere to the provisions of the company's "Information Security Management Policy."
5. All personnel of the company, upon becoming aware of information security incidents or potential violations of the company's "Information Security Management Policy" or related information security regulations, shall report to internal and external units in accordance with relevant internal regulations, respond to the situation, and analyze the root cause to prevent recurrence.
6. The company complies with relevant internal and external regulations, establishes corresponding control procedures, and regularly conducts information security audits to ensure the continuous and effective operation of the information security management system.

The issuance of this statement explicitly declares the company's emphasis on information security. All suppliers, including their full-time and temporary employees, should thoroughly understand the information security statement to safeguard the company's information security.