XXX系統委外開發合約書

|  |  |  |
| --- | --- | --- |
| 立合約書人： | 群益金鼎證券股份有限公司 | （以下簡稱甲方） |
|  | XXXXX股份有限公司 | （以下簡稱乙方） |

茲為系統委外開發事宜，甲方委託乙方開發XXX系統暨技術引進（以下簡稱本專案）之事宜，雙方本誠信原則，訂立本契約，內容如附件所列之系統規格及功能明細，雙方願於本合約有效期間，共資遵循內容如下：

# 專案名稱及內容

### 名稱：群益金鼎證券股份有限公司XXX系統開發暨開發技術引進專案。

### 專案內容及時程：詳如附件一XXX系統開發工作說明書。

# 服務範圍

### 甲方委託乙方完成本專案之進行，乙方同意受託，並應就本專案之範圍、工作內容、使用之技術、所需之人員、時程、成本、交付內容與驗收方式等向甲方提出說明，並以書面提供甲方。

### 乙方提供系統開發工作說明書應包含以下項目，並由乙方負責執行、交付：

##### 甲方需求產品/服務

##### 開發規劃建議

##### 開發規格說明

##### 系統設計與分析

##### 程式設計與開發

##### 系統開發技術之教育訓練工作

##### 測試、安裝、訓練、技術文件提供

##### 乙方符合甲方資安要求之佐證，例如：不低於券商公會資通系統安全防護基準自律規範之乙方資安政策或國標標準認證。

##### 乙方具備專案管理能力之佐證，例如：具有至少一張有效期間內之專案管理相關證照或相關成功專案簡述。

### 上述工作說明書經甲方核定後，應列入本合約之附件項目。

### 乙方於自行發現程式漏洞、版本老舊，或於使用相同服務之其他證券商應用系統發生故障或異常時，應儘速瞭解原因，主動轉知及提供甲方因應措施，俾採取適當程序防範潛在異常事件。

# 合約期限

自民國\_\_\_年\_\_\_月\_\_\_日起至民國\_\_\_年\_\_\_月\_\_\_日止，期間應完成XXX系統開發工作說明書所列之交付項目與驗收。

# 開發費用

本專案之費用總計新台幣（以下同）共計\_\_\_\_\_\_\_\_\_\_元整（含稅）。

# 費用支付

甲方依據乙方提出之付款發票（Invoice），開立整票期為\_\_\_\_\_天之支票支付乙方，並由乙方提供正式收據予甲方。

### 第一期款於本合約簽署後支付，金額為合約總價之百分之三十，計新臺幣X萬X仟元整。

### 第二期款於XXXX階段完成並驗收交付後支付，金額為合約總價之百分之四十，計新臺幣X萬元整。

### 第三期款於XXXX階段完成並驗收交付後支付，金額為合約總價之百分之二十，計新臺幣X萬元整。

### 最後款項於專案完成交付驗收後支付，金額為合約總價之百分之十，計新臺幣X萬元整。

# 服務水準

甲乙雙方約定之服務水準指標如下：

### 客服支援時段

### (一)、乙方同意於系統開發期間固定於每週五與甲方進行系統開發進度檢討報告，並就甲方專案範圍內作業項目提供諮詢服務，並提出下週預定開發進度。

### 問題支援方案

### (一)、乙方同意於本合約全案驗收完成之翌日起一年內（即維護期間），免費負責本系統之除錯責任工作，並提供甲方除錯後之版本。

### (二)、合約標的物如有任何資通安全相關漏洞，乙方應負修補之責，並不得收取任何費用。

### (三)、於維護期間內，乙方同意於接獲甲方系統故障通知時起四個工作小時內派遣工程師至前甲方服務地點進行系統除錯工作，並於八個工作小時內完成除錯後之版本提供並確保系統上線正常運作。

### 每月可歸責於廠商之D級事件之件數上限

### (一)、每月可歸責於乙方之D級以上事件不得連續2個月高於2(含)件，如有逾越，則依第十條合約罰則與終止章節之規定辦理。(D級事件定義請參考本公司「SO-18-001\_事件管理程序」之規範)

### 其它服務水準要求

### (一)、乙方同意於系統開發期間，所有程式之存取皆遵守甲方程式測試、上線流程之規定。

### (二)、涉及核心資通系統與資通服務之專案合約，乙方應於簽約時提供資通系統與資通服務之回復計畫，如以災難復原計畫、備援演練、營運持續計畫等形式呈現。

### (三)、乙方於程式上線前應完整測試。交易主機應設立備援機制，禁止於開盤前及開盤期間進行系統更新及下載，避免客戶端發生重大系統異常。

### (四)、乙方應依前述約定之服務水準指標，每年至少提供一次服務水準報告予甲方確認。

### (五)、如有違反以上服務水準指標應依本合約罰則與終止之規定辦理。

# 乙方以外供應商

### 乙方不得將本約附件一XXX系統開發工作說明書，所定義之工作項目內容轉包或分包予其他供應商。

### 乙方轉包或分包予其他供應商之行為違反本約規定，甲方得向乙方提出解除或終止合約之要求，乙方不得拒絕，如因此致生損害於甲方，甲方得向乙方提出損害賠償之請求。

# 交付項目

乙方須交付“XXX系統開發工作說明書”及合約附件所列之交付項目內容予甲方。

# 驗收內容

### 驗收標準：除依附件一XXX系統開發工作說明書，有關交付項目之說明為依據外，應請乙方提供以下文件說明：

##### 須提列安裝程序、變更、編譯/過版程序、復原程序及作業手冊或操作手冊文件。

##### 乙方交付之程式需經過驗證程序(如：MD5、SHA256)。

##### 須提列所有程式與相關檔案名稱及其所在之目錄，並詳列檔案目錄權限，同時對重要（含機密或敏感性資料）檔案予以標示說明。

##### 須提列原始程式碼版本清單及所存放之目錄名稱，以對原始程式碼做存取權限與變更過版之控管。

##### 須提列應用系統使用者代碼及權限清單，針對使用者之職能詳列其所擁有之權限範圍（不得有職能衝突之情形），包括對資料之增刪修改、列印及程式之執行。

##### 須提列應用系統安全相關測試之書面報告，包括資料輸入檢驗測試，以及參照所提列的「使用者代碼及權限清單」，做權限、功能及邏輯之測試。

##### 須提列作業系統上所有的使用者及群組清單，並詳列其權限、功能。

##### 須提列作業系統的安全維護清單，詳列所需工具、修補程式及其來源、執行步驟與檢驗方式。

##### 須提列必要之網路服務項目及各服務可取存之使用者清單，未列示之網路服務項目將予以關閉。

##### 須提列必要之IP連結清單，連接到主機及資料庫的IP位址將予以管制。

### 程序：驗收標準所列之交付項目，如不符甲方要求，乙方應於收到通知之翌日起三日內改善，並再提交甲方驗收。修改後之交付項目，其驗收程序均適用之。驗收時甲方應提供諮詢與排除系統錯誤之協助。

# 合約罰則與終止：

### 凡任何一方未依本約之規定履行應盡之義務者，即視為違約。

### 乙方未依照“第六條服務水準”內容，甲方有權利扣除本合約總額的百分之一之費用，並於當期維護費款項中扣除。

### 乙方未依合約規定，未能於規定之工作時數內提供並確保系統上線正常運作時，則每逾一小時乙方需賠償甲方本合約總價款千分之五之費用，最高賠償金額不得高於本合約總價。甲方有權利得以書面通知乙方終止合約，不受「合約標準條款」“合約終止處理方式”第三項內容，應於一個月前以書面通知乙方之限制，並返還甲方已支付之維護費用。

### 乙方之違約行為或可歸責於乙方之行為，所致甲方之損害，甲方得請求賠償。該損害賠償數額最高不逾該合約報酬之總金額。

### 乙方之資料存取不當行為或可歸責於乙方之行為，所致甲方之客戶個人資料（指個人資料保護法所明訂之個人資料）遭受外洩時，甲方得請求賠償。該損害賠償數額不受合約報酬之總金額限制。若因此導致第三方發生損害時，乙方應與行為人負連帶賠償責任。

### 乙方如涉及違反其永續發展政策，且對環境與社會有顯著影響時，甲方得隨時終止或解除本契約之條款，乙方並不得向甲方請求任何賠償。

### 雙方承諾不得直接或間接向任何人收取或收受本契約範疇以外之任何形式之不正當利益，如有任何實際或可能違反本條款之情形，任一方須立即書面通知他方。若乙方有違反本條款之虞，甲方得立即終止本合約且無須負擔任何責任。

# 合約附件

本合約之附件為本合約之一部份，與本合約具同一效力。

附件一：「合約標準條款」

附件二：「資訊安全政策聲明」

附件三：「個人資料保護政策聲明」

附件四：「委外(第三方)作業人員保密承諾書」

附件五: 供應商人權及環境永續條款承諾書

附件六:「XXX系統開發工作說明書」

附件七：「資安證照」(依服務範圍需求提供)

附件八：「品質證照」(依服務範圍需求提供)

附件九：「安全性檢測證明」(依服務範圍需求提供)

附件十：「第三方程式元件之來源與授權證明」(依服務範圍需求提供)

立合約書人：

|  |  |  |
| --- | --- | --- |
| 甲方 | ： | 群益金鼎證券股份有限公司 |
| 代理人 | ： | 李文柱 |
| 統一編號 | ： | 22956035 |
| 地址 | ： | 台北市105松山區民生東路三段156號11樓 |

|  |  |  |
| --- | --- | --- |
| 乙方 | ： | XXXXX股份有限公司 |
| 法定代理人 | ： | XXX |
| 統一編號 | ： | XXXXXXXX |
| 地址 | ： | XXXXXXXXXXXXXXXXXXXXXXXXXX |

中華民國xxx年xx月xx日

附件一：合約標準條款

# 責任

### 甲乙雙方於進行本專案過程中，應密切協調配合，以確保本專案之適用性，完整性並如期完成。

### 乙方應負之責任

##### 依各階段服務之規劃，選派適當人員至甲乙雙方同意之指定地點負責進行本專案之執行。

##### 依本合約之約定，完成本專案各階段工作，並依約交付文件。

### 甲方應負之責任

##### 提供乙方相關配合事項及支援，依乙方之要求儘速並及時作出決定、確認及取得所須之管理階層核准，以利本專案之執行。。

##### 依付款規定，撥付乙方費用。

# 專案管理

### 本專案執行期間，甲方應成立專案小組，由本專案相關部門指派人員參與，並由參與人員中指派一名專案協調人，以利本專案協調。本專案執行期間內，所有配合項目均應由專案協調人或由專案協調人指派專案組員與乙方之專案經理或專案經理指派專案人員互為此工作項目之連絡窗口。

### 本專案執行期間，甲乙雙方之專案有關人員應本著誠意原則，俾使本建置順利完成。

# 權利歸屬

### 乙方依本約提供甲方服務時，所產生、取得或持有甲方之資料，包括文字、影像、圖形、聲音，不論其儲存於印刷、磁性、光學或其他媒體上，皆屬於甲方所有。除非為提供服務所需，或經甲方書面同意，不得複製、揭露或交付第三人。

### 乙方為甲方所開發之系統程式，不得違反相關法令或侵害他人權利，若有違反，甲方得拒絕驗收或支付費用，乙方除應將甲方已支付之費用全數返還外，相關法律責任並應由乙方自行負責。

### 甲方於付清所有合約款項後，保有對系統程式的修改權。

# 責任限制

### 乙方保證本合約交付項目之內容，並無任何抄襲或仿冒之情事。未侵害他人之權利，且具有甲方要求之品質。

### 乙方保證依本約提供之標的物內容絶無侵害他人的智慧財產權，如有任何第三人就甲方依本契約約定對使用標的之利用向甲方主張排除之權利，乙方於接到甲方通知後應主導抗辯及有關之和解談判，並自費為甲方提出抗辯及支付所有經法院判決確定的費用及損害賠償。

### 若有權利或品質上之瑕疵，經定期催告而乙方不能或不為處理時，甲方在契合約期間得隨時按下列方式擇一處理。如因此致生損害於甲方者，乙方並負損害賠償責任。

##### 由甲方自費修改瑕疵或取得他人授權，相關費用由乙方負擔。

##### 按瑕疵之程度，減少或收回合約價款。

##### 解除或終止合約。

# 個人資料保護

### 乙方就《個人資料保護法施行細則》應採取以下必要措施：

##### 配置管理之專責人員及相當資源。

##### 界定個人資料之範圍。

##### 個人資料之風險評估及管理機制

##### 事故之預防、通報及應變機制。

##### 個人資料之蒐集、處理及利用之內部管理程序。

##### 資料安全管理及人員管理。

##### 認知宣導及教育訓練。

##### 設備安全管理。

##### 資料安全稽核機制。

##### 使用紀錄、軌跡資料及證據保存。

##### 個人資料安全維護之整體持續改善。

### 如乙方發生個資外洩事件時（如駭客入侵、病毒攻擊或乙方之內部人員盜用等），應立即查明事實後採取降低負面因應對策，並於第一時間告知甲方（告知事項應包括但不限於第三人非法獲知方式、建議降低客戶被影響之措施、採取之解決機制（包含解決時程、程序及措施）。

### 如有任何第三人向甲方提出個人資料外洩之訴訟時，若該個人資料之蒐集、處理及利用與乙方有關者，乙方應配合提供資料保護善良管理之證明

# 資訊安全

乙方若不涉及程式開發則請遵守第五項，若有則請全部遵守。

### 程式原始碼安全

### 甲方無法取得乙方為甲方所開發之系統程式原始碼時，乙方應保證其為甲方所開發之系統程式符合安全事項，包含：

##### 程式應避免含有惡意程式等資訊安全漏洞，如OWASP TOP 10、CWE/SANS TOP 25、木馬程式、後門、間諜程式、資料庫隱碼等漏洞皆不可存在。檢查程式碼後，如發現有安全漏洞或後門程式，則須立即進行補強。

##### 於每次程式異動上線時需提供資安檢測報告書(含源碼檢測、弱點掃描)。

##### 就甲乙雙方所提供之相關檢測報告紀錄，乙方須負檢測報告內標註中、高風險程式碼修改之責任及低風險建議與保護措施說明。

##### 合約期間內須定期評估系統所使用之外部元件或軟體之安全性漏洞及提供相關資訊，並配合本公司進行滲透測試、弱點掃描作業，檢測後若需調整網頁程式，須於雙方議定之時限內，完成弱點、漏洞補強。

##### 程式應使用適當且有效之完整性驗證機制，以確保其完整性。

##### 如需引用第三方函式庫，應辦理風險評估且建立前揭函式庫清單及版本管控機制(例如：有新增使用或異動版本時，應留意該函式庫是否有已公告之安全性漏洞(CVE)並留存紀錄)，並揭露第三方程式元件之來源與授權證明，方可使用。

##### 程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。

##### 程式規劃設計時納入隠私保護機制

##### 使用者驗證資訊須以加密方式傳遞，倘於系統上線前受通報加密方式具無法修復之資安弱點，則雙方得另行議定加密方式。

##### 資通系統應遮蔽鑑別過程中之資訊，且系統發生錯誤時，使用者頁面僅得顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息，詳細錯誤訊息留存於系統日誌內供維運除錯使用。

##### 設計階段依系統功能及要求，需設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形。

##### 系統開發須遵循安全系統發展生命周期(SSDLC)準則，並於系統發展生命週期將各階安全需求(含機密性、可用性、完整性)納入考量。

### 行動應用程式安全

##### 行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。

##### 應於發布前檢視行動應用程式所需權限與提供服務相當，首次發布或權限變動應經甲方資安、法遵單位同意，並留有紀錄，以利綜合評估符合個人資料保證護法之告知義務。

##### 行動應用程式傳送及儲存敏感性資料時應透過憑證、雜湊（Hash）或加密等機制以確保資料傳送及儲存安全，並於使用時應進行適當去識別化，相關存取日誌應予以保護以防止未經授權存取。

##### 啟動行動應用程式時，如偵測行動裝置疑似遭破解（如root、jailbreak、USB debugging等），應提示使用者注意風險，乙方免費提供程式偵測之調整；亦應提示使用者於行動裝置上安裝防護軟體及APP於模擬器安裝執行時之安全性提醒。

##### 行動應用程式於初次上架前及每年，甲方委由經財團法人全國認證基金會(TAF)認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以經濟部工業局委託執行單位「行動應用資安聯盟」公布之「行動應用程式基本資安檢測基準項目」進行檢測。乙方須負報告公版檢測脆弱點修復之責，最遲於3個月內完成修復且通過「行動應用App基本資安檢測報告」完成後方可上架。

##### 通過實驗室檢測後一年內有更新上架之需要，應於每次上架前，乙方就重大更新項目進行委外或自行檢測通過，並將相關檢測記錄交付甲方；所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。檢測範圍以OWASP MOBILE TOP 10之標準為依據，留存相關檢測報告紀錄，須負檢測報告內標註高風險程式碼修改之責及中低風險建議與保護措施說明。

##### 行動應用程式（APP）引用第三方函式庫，應辦理風險評估且建立前揭函式庫清單及版本管控機制(例如：有新增使用或異動版本時，應留意該函式庫是否有已公告之安全性漏洞(CVE)並留存紀錄)，並提供甲方第三方程式元件之來源與授權證明，方可使用。

### 乙方若須使用行動碼（Mobile Code）應符合本公司資訊安全規範之要求。如因此對甲方造成損害者，乙方應負損害賠償責任。

### 乙方交付之程式應提供安全性檢測證明(如行動應用程式資安檢測、源碼檢測、弱點掃描等)，並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試，乙方若無法取得安全性檢測證明，則應提供資安聲明書，以確保其交付之產品無安全性漏洞。

### 資通安全事件通報與調查

##### 乙方應就受託業務建立資通安全事件通報機制，並對專案成員實施資通事件通報演練或相關宣導作業，使專案團隊成員了解通報流程及資通安全相關法令規定。乙方於違反資通安全相關法令規定或知悉資通安全事件時或發現存有任何潛在問題和危害而有影響受託業務之虞者，應立即通知本公司並採取相關補救措施。

##### 乙方如發現有關資通安全事件，應立即通報本公司相關負責人員。乙方需配合本公司，進行所發生安全事故之調查及蒐證。

# 乙方服務團隊之規範

### 乙方應根據本約內所應提供之服務，於本約生效後五個工作日內組成專業與完整之服務團隊並提出服務團隊成員名冊，交由甲方認可。服務團隊成員名冊應註明：服務人員之職稱、個人履歷、與負責之工作。如甲方有正當之理由，得拒絕乙方所提供之服務成員。乙方應於收到甲方拒絕通知5個工作日內，完成甲方所接受之替代人員補充。乙方團隊成員之增補亦適用以上規定。乙方團隊主管應為專任，不得參與本契約規定以外之工作。

### 乙方團隊成員異動時，應於五個工作日內通知甲方，更新乙方團隊成員資訊。

### 乙方進駐甲方之人員應簽署《委外（第三方）作業人員保密承諾書》、《委外（第三方）作業人員進駐之工作規範》、《資訊安全政策聲明》、《個人資料保護政策聲明》。

### 乙方派駐甲方之人員應遵守甲方內部之管理規定、在穿著談吐舉止上保持專業之形象，與甲方人員交往範圍不應超越工作上之需要。

### 乙方依本約規定提供服務，應對其聘雇之團隊成員善盡監督責任，並應自行負責相關法令所規定雇主對員工之責任與義務，包括但不限於工作人員之勞工安全衛生責任，如乙方人員有任何傷害或死亡之情形發生，概由乙方負責，與甲方無涉。如因此致生損害於甲方或致甲方受相關處分時，應由乙方賠償之。

### 甲方如認為乙方團隊成員有違背契約規定或其他不適任之情事者，可以口頭方式通知乙方聯絡人，轉知並告誡該成員限期改正。如甲方以書面敘明具體理由，要求乙方團隊成員離任時，被要求離任之乙方團隊成員，應於收到書面當日下班前離任。

# 合作資訊供應商(策略聯盟)供應商存取控制

乙方若為合作資訊供應商，乙方應遵守以下必要措施：

### 串接方式，交易相關只能透過群益提供之H5網頁登入、下單 ; 公開資訊則可使用OPENAPI提供串接。

### 客戶任何與群益互動資料請求，其傳送路徑不得透過任何方式保存取得之資料。

### 群益所提供的H5為獨立網頁，不得再提供token或API等免登入的驗證方式。

### 合作供應商所開發之產品無儲存群益客戶之交易帳密的行為。

# 物聯網設備採購

乙方所提供之產品如屬物聯網設備，乙方應遵守以下資訊安全性協議：

### 應協助變更所提供之物聯網設備之初始密碼，關閉物聯網設備不必要之網路連線及服務，針對開放網路連線之服務埠號，廠商須提供相關說明文件。

### 所提供之物聯網設備應提供安全性更新機制且定期更新，如存在已知弱點無法更新時，應建立補償性管控機制。

### 乙方應主動通報設備已知資安漏洞並提出相關應變處置方案，確保設備不存在已知安全性漏洞。

### 需配合甲方每年物聯網設備弱掃發現弱點的修補，或提供修補作法予以甲方。

### 乙方執行物聯網設備進駐與維護作業時，應依甲方規範駐點人員辦法，塡寫維護紀錄或簽署資安承諾文件等，以利後續作行為追蹤及保障。

### 乙方於物聯網設備提供時，應交付相應之操作或說明文件，並就所提供之物聯網設備應檢附相應之資訊安全檢測證明，以茲佐證其產品安全性(如:弱點掃描測試或原廠安全更新文件等)。

# 違約責任

### 凡任何一方未依本約之規定履行應盡之義務者，即視為違約。

### 乙方如有下列任何一種情事者，當然視同違約：

##### 聲請或被聲請重整、解散或決議解散或被命令解散或裁判解散。

##### 依破產法為和解，或聲請或被聲請宣告破產。

##### 主要資產被查封、顯無清償能力。

##### 遭受法院查封、假扣押、假處分、保全處分、強制執行程序、開始重整程序以致無法履行本約義務者。

##### 發生票據退票之情事或遭受停止付款處分或有受停止付款處分之虞者。

##### 結束營業、暫停營業、大規模解雇職工、或有相當事實足證乙方有發生上述情事之虞者。

##### 合併或決議合併、變更其營業、有第三人接管理其營業，或其所為之聲明、承諾或保證經證明為不實，且因而影響乙方履行本約之能力者。

##### 合併後存續之公司或法律實體或接管其營業之第三人，未以書面承諾無條件完全承受乙方依本約所負之義務或責任者。

##### 乙方變更其營業內容，像主管機關申報刪除其有關資訊服務之營業項目者。

### 乙方之違約行為或可歸責於乙方之行為，所致甲方之損害，乙方應負賠償責任。

# 乙方以外供應商

### 乙方不得將本約工作內容轉包或分包予其他廠商。

### 乙方轉包或分包予其他供應商之行為違反本約規定，甲方得向乙方提出解除或終止合約之要求，乙方不得拒絕，如因此致生損害於甲方，甲方得向乙方提出損害賠償之請求。

# 乙方之保證

### 乙方保證依本約提供之標的物內容絶無侵害他人的智慧財產權，如有任何第三人就甲方依本契約約定對使用標的之利用向甲方主張排除之權利，乙方於接到甲方通知後應主導抗辯及有關之和解談判，並自費為甲方提出抗辯及支付所有經法院判決確定的費用及損害賠償。

### 乙方處理甲方委託事項時應確實遵守個人資料保護法等相關法令規定。

### 乙方係依中華民國公司法成立並存續之公司，並依法令規定得提供本約各項服務。

### 乙方已依照其內部程序規定簽署本約。

### 乙方在參與甲方標案時，所提供之資料，均為完整且真實無誤。

### 乙方已充分瞭解本契約之內容並自願全部遵守履行，未來不得以任何可能影響履行本約履行之事由、主張、或事故請求或主張部分或全部免除本約履行之責任。

### 乙方應自主實施相關人權政策教育訓練，並簽署甲方所提供之「供應商人權及環境永續條款承諾書」。

### 乙方(供應商)如涉及違反其永續發展政策，且對環境與社會有顯著影響時，甲方(本公司)得隨時終止或解除本契約之條款，乙方(供應商)並不得向甲方(本公司)請求任何賠償。

### 雙方承諾不得直接或間接向任何人收取或收受本契約範疇以外之任何形式之不正當利益，如有任何實際或可能違反本條款之情形，任一方須立即書面通知他方。若乙方代理商、供應商)有違反本條款之虞，甲方本公司得立即終止本合約且無須負擔任何責任。

### 若屬營繕工程類、設備用品類合約應增加如下條款：

### 乙方所提供之產品(原物料)標準，宜符合政府認可之環保、節能、節水及綠建材標章等之綠色產品；或符合再生材質、低污染、可回收、省資源、其他可增加社會利益或減少社會成本，而效能相同對環境衝擊較少之環保產品。

### 若屬物聯網設備採購（含租賃）或維護合約應增加如下條款：

### 乙方供應商所提供之產品如屬物聯網設備，乙方應遵守以下必要措施：

### 應協助變更所提供之物聯網設備之初始密碼。

### 所提供之物聯網設備應具備安全性更新機制且定期執行更新，如存在已知弱點無法更新時，應建立補償性管控機制與說明。

### 應關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。針對開放網路連線之服務埠號，廠商須提供相關說明文件。

### 應主動通報乙方提供甲方之物聯網設備已知資安漏洞並提出相關應變處置方案，確保設備不存在已知安全性漏洞。

### 乙方供應商所提供之物聯網設備，宜優先採用取得資安標章之物聯網設備。

### 乙方供應商執行物聯網設備進駐與維護作業時，應提供甲方本公司維護紀錄或資安承諾文件等，以利後續作行為追蹤及保障。

### 乙方供應商於物聯網設備提供時，應交付相應之操作或說明文件，並就所提供之物聯網設備應檢附 相應之弱點掃描報告或聲明文件，以茲佐證其產品安全性。

### 除上述之聲明與保證外，甲方或乙方均未以明示或暗示之各種方式聲明與保證在此之外之任何事項。

# 乙方作業之服務與稽核

### 甲方得每年至少一次或於知悉資訊服務供應商發生可能影響其委託業務之資通安全事件時，自行派員或授權第三方檢查或稽核乙方提供之服務是否符合本約規定之權利，乙方應以合作之態度在合理時間內提供甲方相關書面資料，或協助約談相關當事人。上述檢查或稽核得以不預告之方式進行之，乙方不得拒絕。

### 委外作業如為一年期以上，乙方應定期或每年至少一次提交服務水準報告予甲方確認。

# 乙方之保密義務

### 乙方承諾於本約有效期間內及本約期滿或終止後，對於所得知或持有一切因甲方執行公權力所必須保有之公務秘密，以及甲方依契約或法令對第三人負有保密義務之業務祕密，均應以善良管理人之注意妥為保管及確保其祕密性，並限於本約目的範圍內，於甲方指定之處所內使用之。非經甲方事前書面同意，乙方不得為本人或任何第三人之需要而複製、保有、利用該等公務祕密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等公務機密，或對外發表或出版，亦不得攜至甲方或甲方所指定處所以外之處所。

### 乙方同意本條所定公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之乙方團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書。

### 乙方及乙方人員違反本條規定時，乙方除應賠償甲方因此所受之損失外，並應給付相當於本約總價款之懲罰性違約金予甲方。

# 爭議處理程序

### 甲乙雙方應本誠信原則履行本約各項規定，如因本約之履行發生爭議而無法由雙方專案負責人協議解決者，就爭議之解決所做之決議有拘束雙方之效力。

### 甲乙雙方無法達成決議之案件，雙方同意以甲方所在地之台灣台北地方法院為第一審管轄法院。並以中華民國之法律為準據法。

# 合約效力

### 本合約及其附件之任何變更、增刪、或修改，經雙方授權代表人簽署以書面換文方式完成後生效。

### 本合約自雙方簽訂之日起生效，取代合約簽訂前雙方所有以口頭或書面之建議、協議或會談。任何於本契約生效前經雙方協議而未記載於本契約之本文或其附件之事項，對雙方均無拘束力。

### 本約部分條款依法被認為無效時，其他條款仍應繼續有效。

### 本合約之附件視為合約之一部分，與本合約有同一效力。但附件與合約抵觸時，以合約本文為準。

# 合約書本

本合約正本一式二份，經甲乙雙方簽署後，正本由甲乙雙方依稅法規定各自貼足印花稅票後收執各一份。

群益金融集團 Capital Group

資訊安全政策聲明

群益金融集團（以下簡稱本集團）秉持維護本集團作業環境之資訊安全理念，對於公司所儲存或傳遞之資料應作周全保護與防範，以杜絕毀損、失竊、洩漏、竄改、濫用與侵權等事故。本集團將定期修訂資訊安全政策，並貫徹執行，以持續提昇各資訊服務系統所有作業之機密性、完整性與可用性。

本集團資訊安全政策如下：

1. 本集團資訊安全措施，應符合法律之規範與本集團資訊安全政策之要求；所有資訊安全控制或程序之開發、修改及建置，須符合並遵循資訊安全管理體系之機制。
2. 本集團所有人員（係指員工、約聘雇人員、協力廠商及顧問）凡其使用本集團資訊以提供資訊服務或執行專案工作等，均有責任及義務保護其所取得或使用本集團之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。所有資訊資產的存取與使用，應經正式授權、存取管制與身份辨識程序。
3. 本集團客戶資料，包含交易資料與基本資料，為公司最高業務機密，嚴禁未經授權存取與洩露。處理客戶資料的主機與系統應有專屬且隔離的網段與電腦作業環境。
4. 本集團資訊資產皆屬公司所有，所有在公司內資訊設備、網路資源上所處理、存有、或往來的資訊歸屬公司財產，公司有權觀看、複製、或取用。
5. 本集團各部處資訊資產管理者，必須對其所負責領域或持有之資訊資產，建置使用狀況之監控程序，以隨時發掘系統或資訊遭濫用的潛在風險，加強資料之機密性、可用性及完整性。
6. 本集團應依業務需求訂定業務持續運作計畫，並定期測試演練，並於市場交易量、業務變化及客戶屬性等發生顯著異動時發動辦理，俾憑評估系統資源調配或擴增，維持其適用性。
7. 工作分派應考量職責分離，職務與責任範圍應予區分，以避免資訊或服務遭未授權修改或誤用。
8. 所有人員對於有發生安全事件、安全弱點及違反安全政策與程序之虞者，應隨時保持警戒，並依程序進行通報。
9. 嚴禁所有人員於公司內部網路上安裝、使用、下載非法或未授權之軟體。
10. 所有人員如未經授權擅自使用資訊系統或違反本資訊安全政策及相關安全規定者，將衡酌情節追訴其法律責任，員工及約聘雇人員倂依本集團人事規章議處。

本聲明之頒布，明確宣示維護資訊安全的重要性，各部處應確實瞭解資訊安全政策，並遵循相關管制作業程序，以維護本集團所有業務之資訊安全與永續經營。

本人已審閱本資訊安全政策內容，茲承諾遵循相關管制作業程序，並簽章如下：

審閱人員： （簽名或蓋章） 職 稱：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

公司名稱（或部門名稱）： 電 話：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

通訊地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日 期： 年 月 日

**群益金融集團**

**個人資料保護政策聲明**

群益金融集團(以下簡稱本集團)秉持落實個人資料保護及管理措施，遵循《個人資料保護法》所述之相關要求及保障個人資料當事人之權利，降低任何個人資料檔案受侵害之事件所可能帶來的衝擊，並持續運作及改善個人資料管理制度，特發布此聲明。

本集團個人資料管理政策聲明如下：

（一） 遵守我國個人資料保護相關之法令規定；

（二） 本公司只會基於合法、正當合理的特定目的，在確實必要的範圍內蒐集個人資料；

（三） 基於合法、正當合理的特定目的蒐集最少的必要個人資料，且不會處理多餘的個人資料；

（四） 本公司會清楚告知當事人，其個人資料將如何被使用及被誰使用；

（五） 已蒐集的客戶資料只會作適當且相關的處理；

（六） 公平合法地處理個人資料；

（七） 維持一份本公司處理的個人資料類別清單；

（八） 確保個人資料的正確性，並於必要時進行更新；

（九） 已蒐集的個人資料將會依法或在合法、正當合理的特定目的下保存；

（十） 尊重當事人對其個人資料所能行使之權利，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除等；

（十一） 以適當安全之水準技術保護其所蒐集、處理、利用之個人資料檔案，確保所有個人資料的安全；

（十二） 只有在確實已有適當充分保護的狀況下，本公司才會將個人資料進行國際傳輸；

（十三） 當個人資料應用於《個人資料保護法》所允許之例外情形時，應確保其適當性與合法性；

（十四） 建立與實施個人資料管理制度並持續維運，讓個人資料保護政策落實，以確保個人資料檔案之安全；

（十五） 鑑別內外部利害關係者及其參與個人資料管理制度治理與運作的程度；

（十六） 於個人資料管理制度運行中，明確界定員工之責任與義務。

（十七） 規劃緊急應變程序以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。

（十八） 如有委託蒐集、處理及利用個人資料時，妥善監督受託機關。

（十九） 設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢。

本聲明之頒布，明確宣示維護個人資料管理的重要性，全體員工應確實瞭解此聲明內容，以維護本集團所有個人資料檔案之安全與永續經營。

本公司承諾遵循上述政策聲明，並簽章如下：

公司名稱：

代 表 人： (簽名或蓋章)

通訊地址：

日 期： 年 月 日

**群益金融集團**

**委外(第三方)作業人員保密承諾書**

立承諾書人 (以下簡稱乙方)參與 「群益金融集團」(以下簡稱甲方）之委託辦理業務或服務(以下簡稱本專案)，為確保於專案執行期間有知悉或可得知悉或持有甲方業務秘密、開發成果、技術秘密及相關文件資料之機密性，並確認智慧財產權歸屬，乙方承諾恪遵下列各項規定。

專案名稱：

本專案之執行期間：自 年 月 日 迄 年 月 日止。

1. 乙方就合於下列或其他情形之資訊，對甲方負有保密義務並採取適當之保密措施：
2. 所有與本專案有關之討論內容、文件、紀錄、圖片、手稿、程式、計畫、資料庫及其他相關資料，包括且不限於以文字、聲音、影像、軟體等形式紀錄者；
3. 甲方以書面或口頭表示，應加保密者；
4. 甲方指定僅供特定人聽閱或利用者；
5. 尚未公開於大眾週知或他人無法依正當合法途徑探知者。
6. 對於前條所定之資訊，非經甲方事前以書面同意，乙方不得為以下任何行為：
7. 提供、交付或以任何方式或因任何原因而公開、洩漏移轉予第三者或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版。
8. 擅自使用於非甲方所指定或委託之工作內容。
9. 擅自拷貝、照相或以其他方法複製全部或部份內容。
10. 以任何方式提供第三人使用或參考，或為任何侵害甲方權益之行為。
11. 承諾於本專案有效期間內及期滿或終止後，對於所得知或持有一切依本承諾書、契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其機密性，並限於本專案有效期間及目的範圍內，於甲方指定之處所內使用之。
12. 專案期間內，非經甲方事前以書面同意，乙方不得從事其他任何與本專案類似或有關連之專案或提供第三人與本專案相關之顧問意見。
13. 為維護甲方機密及相關業務個人資料保護，乙方因本承諾書所負之保密義務，不因乙方轉換公司、工作單位或僱傭關係終止、撤銷、無效或不成立而失其效力。
14. 若甲方將該等開發成果或技術秘密對外公開或解除其機密性者，乙方亦同時解除對該等開發成果或技術秘密之保密責任。
15. 乙方同意於參與本專案期間，因執行本專案所產生或創作之構想、概念、發現、發明、改良、公式、程序、製造技術、著作及相關開發成果，皆屬本專案之成果。無論有無取得專利權、著作權或其他權利及其衍生利益均歸甲方所擁有。
16. 乙方保證本專案期間，絕無任何侵害他人智慧財產權或剽竊他人成果或技術之行為，若有任何違法情事，應自行承擔一切相關之法律責任。如甲方因此而涉訟，乙方應協助甲方解決訴訟紛爭，並負擔所有損害賠償責任。
17. 乙方如於本專案開發期間完成之專利與其他著作，乙方應立即通知甲方以確認各項權利歸屬。
18. 若甲方認為有必要對上述創作申請或登記國內、外相關權利，乙方同意無償協助甲方完成之。
19. 文件資料所有權

乙方同意所有記載甲方資料之文件或其影本、儲存媒體等皆屬於甲方所有，專案終止後，應將佔有之相關資料返還甲方。倘資料為系統軟體等電磁紀錄時，乙方並承諾切實執行系統軟體及電磁紀錄之移除或消磁作業。

1. 立書人保證知悉甲方內部重大資訊時，不得洩露所知悉之甲方內部重大資訊予他人。
2. 立書人保證不得向知悉甲方內部重大資訊之人探詢或蒐集與個人職務不相關之甲方未公開重大資訊，對於非因執行業務得知甲方未公開之重大資訊亦不得向其他人洩露。
3. 個人資料保護：

乙方團隊成員人員，應嚴守工作保密義務與相關法令對業務機密負完全保密之責，尊重「個人資料保護法」之相關規定，並依循甲方有關資訊安全及個人資料保護安全之規定，絕不擅自蒐集、複製、利用及傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有個人資料，僅於受託契約業務範圍內蒐集、處理或利用個人資料。

1. 本承諾書不因本專案期滿或終止後即失其效力，乙方擔保乙方之受僱人、受任人、代理人、繼受人及受讓人等，均亦遵守本承諾書之所有條款，如有違反應自負民事、刑事責任；如造成甲方或第三者之損害，乙方同意無條件負擔全部所有責任，包括但不限於因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。如第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方願意充份合作並提供。
2. 本承諾書之效力與其釋義應遵循中華民國相關法律。如有衍生爭議與訴訟，應以台北地方法院為第一審管轄法院。

|  |  |
| --- | --- |
| 立書人： （簽名或蓋章） | 職稱： |
| 公司名稱： |  |
| 身分證字號： |  |
| 通訊電話： | |

中華民國 年 月 日

**群益金鼎證券股份有限公司   
附件五：供應商人權及環境永續條款承諾書**

群益金鼎證券股份有限公司為落實環境永續理念及履行企業社會責任，特對供應商之人權政策、環境永續政策及行為準則政策等事項為宣導，期望共同遵循與實踐。

**人權政策**

1. 供應商於職場人權保障應致力於營造一個多元、開放、平等且免於騷擾的工作環境，絕不允許任何違反人權行為，如雇用童工、強迫勞動等，亦絕對禁止因個人性別、性傾向、種族、階級、年齡、婚姻、語言、思想、宗教、黨派、籍貫、出生地、容貌、五官、身心障礙或以往工會會員為由，而為差別待遇或任何形式之歧視；此外，供應商亦應提供多元且安全之申訴管道，保障員工合法權益免受侵害。
2. 供應商於職場安全與健康促進方面，除恪遵各項勞動法令規範外，並致力於建構健康、安全與舒適之職場環境。
3. 供應商應尊重員工籌組及加入各類社團組織之權利，勞資溝通方面，除定期辦理勞資會議代表選舉，召開勞資會議外，並提供多元化的溝通機制及平台，確保和諧雙贏的勞資關係。

**環境永續政策**

1. 供應商所提供之產品(原物料)標準，宜符合政府認可之環保、節能、節水及綠建材標章等之綠色產品；或符合再生材質、低汙染、可回收、省資源、其他可增加社會利益或減少社會成本，而效能相同對環境衝擊較少之環保產品。
2. 對於可能釋放到環境中造成危害之物料，供應商應先加以辦識與管理，並於製程、儲存、廢棄物處理等過程中，對環境賦予保護與管理之責。
3. 供應商應進行溫室氣體盤查及規劃制定相關碳管理措施，以降低對環境的衝擊。

**行為準則政策**

1. 供應商承諾不得直接或間接向任何人收取或收受契約範疇以外之任何形式之不正當利益，如有任何實際或可能違反本條款之情形，須立即書面通知。若供應商有違反本條款之虞，本公司得立即終止本合約且無須負擔任何責任。
2. 供應商如涉及違反其永續發展政策，且對環境與社會有顯著影響時，本公司得隨時終止或解除契約之條款，供應商並不得請求任何賠償。
3. 供應商承諾遵守智慧財產權及相關法律。

綜上，敬請供應商確實遵守與實踐上述各項企業社會責任事項及相關法律，如於執行時發現缺失，請立即採取必要之糾正措施，以落實並持續改進。

簽署供應商名稱： (請加蓋公司大章)

中 華 民 國 年 月 日