；

資訊服務供應商委外風險管理作業程序

|  |  |
| --- | --- |
| 文件編號： | SO-02-002 |
| 文件版次： | V 3.7 |
| 發行日期： | 2025/02/12 |

文件修訂履歷

| 修訂版次 | 修訂日期 | 發行與變更說明 | 修訂人員/單位 | 核准 人員 |
| --- | --- | --- | --- | --- |
| V1.0 | 2005/12/08 | 新版文件發行 | 郭資深副總裁美伶 | 郭資深副總裁美伶 |
| V1.1 | 2005/01/26 | 1. 修改第一節：一：2：增加合約審核作業流程，請參考《SO-02-002-F05合約審核作業流程圖》。 2. 修改第二節：二：派駐人員或委外第三方應簽立《SO-02-001-F01委外（第三方）作業人員保密合約》、《SO-02-001-F02委外（第三方）作業人員進駐之工作規範》、《SO-02-001-F03資訊安全政策聲明》。 3. 修正第七章輸出文件記錄內容 | 周宗亮 | 郭資深副總裁美伶 |
| V1.2 | 2008/08/12 | 修正資訊安全管理委員會名稱為營運持續暨資訊服務委員會以因應BS25999與ISO20000導入。 | 陳鑫如 | 梁資深副總裁維誠 |
| V1.3 | 2009/09/04 | 1. 新增資訊服務管理體系角色供應商管理主管及供應商管理流程負責人權責及相關作業內容。 2. 修訂第三章名詞解釋。 3. 修訂第四章相關文件。 4. 因應流程變更，修訂《SO-02-002-F05合約審核作業流程圖》。 5. 原二階文件資訊委外暨第三方存取管理規範（SC-00-002）附件 6. 系統委外開發合約書範本 7. 維護合約書範本 8. 設備採購暨系統整合服務合約書範本 9. 移至本管理辦法並變更表單編號 10. 修訂第六章第一節第一點增列合約金額100萬以上之要求。 11. 新增附件《SO-02-002-F09合約檢核清單》。 12. 廢止附件《SO-02-002-F03委外第三方或下包廠商電腦資源申請表》、《SO-02-002-F04委外第三方存取資料申請單》改由申請人填寫需求申請單進行申請。 | 陳鑫如 | 梁資深副總裁維誠 |
| V1.4 | 2009/11/02 | 修訂第六章第三節。針對當年度有履約之廠商及50萬元以上採購廠商進行供應商審查。 | 陳鑫如 | 梁資深副總裁維誠 |
| V1.5 | 2009/12/11 | 1. 修訂第五章角色與權責。 2. 統一名詞: 3. 統一將供應商或契約調整為合約 4. 統一將廠商調整為供應商。 5. 修訂第六章第三節三，述明供應商滿意度調查啓動及後續追蹤作業權責。 | 陳鑫如 | 梁資深副總裁維誠 |
| V1.6 | 2009/12/24 | 1. 修訂第六章第三節專案管理，增列金額100萬（含）以上之合約。專案負責人應填寫《SO-02-002-F10供應商支援紀錄表》，並依服務提供狀況作為供應商滿意度調查參考。 2. 新增《SO-02-002-F10供應商支援紀錄表》。 | 陳鑫如 | 梁資深副總裁維誠 |
| V1.7 | 2010/11/5 | 因應個資法修訂，加強合約條文中對委外廠商之損害賠償責任及配合舉證責任之要求，修訂《SO-02-002-F06系統委外開發合約書範本》、《SO-02-002-F07維護合約書範本》、《SO-02-002-F08設備採購暨系統整合服務合約書範本》 | 陳鑫如 | 劉副總裁淑如 |
| V1.8 | 2011/10/21 | 1. 因應公司更名，修訂文件公司名稱。 2. 同步修訂附件1、6、7、8。 | 陳鑫如 | 劉經理昭慧 |
| V2.0 | 2011/11/18 | 因應公司文件核准層級，文件名稱配合變更。 | 藍曉萍 | 劉經理昭慧 |
| V2.1 | 2013/05/06 | 因應ISO20000:2011新版條文要求，修改第六章作業內容與委外第三方簽訂合約之安全要求中供應商審查之條件（50萬元以上改100萬元以上）說明。 | 周杰澐  方學豪 | 周資深經理宗亮 |
| V2.2 | 2013/10/24 | 因新增《SO-02-001-F04期貨委外(第三方)作業人員保密合約》，修訂第六章第二節、第七章相關內容。 | 簡嘉慧 | 周資深經理宗亮 |
| V 2.3 | 2013/11/14 | 1. 因《SO-02-002-F02臨時服務證申請單》與《SO-03-001-F02臨時服務證申請單》相同，廢除前者，統一採用後者。 2. 於第七章中補列《SO-02-002-F10\_供應商支援紀錄表》。 | 方學豪 | 周資深經理宗亮 |
| V2.4 | 2014/01/23 | 原《SO-02-002-F05\_合約審核作業流程圖》更改代號為《SO-02-002-附件A\_合約審核作業流程圖》。 | 方學豪 | 周資深經理宗亮 |
| V2.5 | 2014/11/04 | 1. 新增《SO-02-002-F11\_供應商營運持續管理評估表》，並修訂第六章相關內容。 2. 修訂《SO-02-002-F07\_維護合約書範本》。 3. 修訂《SO-02-002-F08\_設備採購暨系統整合服務合約書範本》。 | 簡嘉慧 | 周資深經理宗亮 |
| V2.6 | 2015/01/12 | 修訂《SO-02-002-F11\_供應商營運持續管理評估表》 | 簡嘉慧 | 周資深經理宗亮 |
| V2.7 | 2016/03/28 | 1. 因應企業社會責任，修訂《SO-02-002-F06\_系統委外開發合約書範本》、《SO-02-002-F07\_維護合約書範本》、《SO-02-002-F08\_設備採購暨系統整合服務合約書範本》 2. 修訂第五章專案負責人權責 3. 修訂第六章駐點人員需簽署文件清單 | 簡嘉慧 | 周資深經理宗亮 |
| V2.8 | 2017/12/28 | 1. 因應企業社會責任，修訂《SO-02-002-F06\_系統委外開發合約書範本》、《SO-02-002-F07\_維護合約書範本》、《SO-02-002-F08\_設備採購暨系統整合服務合約書範本》 2. 新增《SO-02-002-F12\_設備採購合約書範本》 | 簡嘉慧 | 周資深經理宗亮 |
| V2.9 | 2018/12/27 | 配合「SO-02-001 委外駐點人員管理程序」修訂，調整「SO-02-002-F06 系統委外開發合約書範本、SO-02-002-F07 維護合約書範本、SO-02-002-F08 設備採購暨系統整合服務合約書範本、SO-02-002-F12 設備採購合約書範本」之「SO-02-001-F01 委外(第三方)作業人員保密合約」。 | 雷雅惠 | 周資深經理宗亮 |
| V3.0 | 2019/1/29 | 配合「SO-02-001 委外駐點人員作業程序」修訂，修改「SO-02-001-F01」附件名稱為「委外(第三方)作業人員保密承諾書」。 | 雷雅惠 | 周資深經理宗亮 |
| V3.1 | 2019/8/15 | 1. 因應群益金融集團辦公室搬遷，修訂「SO-02-002-F06 系統委外開發合約書範本」、「SO-02-002-F07 維護合約書範本」、「SO-02-002-F08 設備採購暨系統整合服務合約書範本」、「SO-02-002-F12 設備採購合約書範本」公司地址及附件名稱資訊安全政策聲明。 2. 修訂「SO-02-002-F09 合約檢核清單」新增文件標頭及簽核欄。 3. 因應「SO-02-001委外駐點人員管理程序」修訂 「SO-02-001-F01委外(第三方)作業人員保密合約」併同修訂合約附件。 | 雷雅惠 | 周資深經理宗亮 |
| V3.2 | 2022/7/11 | 參考「證券暨期貨市場各服務事業供應鏈風險管理參考指引」，新增第六章第五節服務終止與解除內容。 | 邱聿莛 | 施雷蜀華 |
| V3.3 | 2023/1/16 | 1.參考「證券商供應鏈風險管理自律規範」，調整相關內容。  2.取消部份輸出表單。 | 陳佳宜 | 施雷蜀華 |
| V3.4 | 2023/5/10 | 1.增加「SO-02-002-F13\_勞務採購契約書範本。」、「SO-02-002-F14\_軟體維護合約書範本」。 | 吳佩芸 | 施雷蜀華 |
| V3.5 | 2023/7/31 | 增加委外作業流程及說明 | 王奎元 | 施雷蜀華 |
| V3.6 | 2024/11/22 | 增加委外作業流程及說明 | 王奎元 | 施雷蜀華 |
| V3.7 | 2025/01 | 1. 配合「證券商資通系統與服務供應鏈風險管理自律規範」修訂調整遴選、合約簽屬及定期審查作業程序。 2. 調整各合約書範本 | 潘世佳 | 施雷蜀華 |

目 錄

[第一章 目的 8](#_Toc186212421)

[第二章 適用範圍 8](#_Toc186212422)

[第三章 名詞定義 8](#_Toc186212423)

[第四章 相關文件 9](#_Toc186212424)

[第五章 權責 9](#_Toc186212425)

[第一節 委外第三方 9](#_Toc186212426)

[第二節 供應商管理流程負責人 10](#_Toc186212427)

[第三節 供應商管理主管 10](#_Toc186212428)

[第四節 本公司專案負責人及專案負責單位 10](#_Toc186212429)

[第五節 法令遵循暨法務室 11](#_Toc186212430)

[第六節 資訊安全人員 11](#_Toc186212431)

[第七節 資訊部主管 11](#_Toc186212432)

[第六章 作業內容 11](#_Toc186212433)

[第一節 資訊服務供應商遴選 11](#_Toc186212434)

[第二節 資訊服務供應商合約 12](#_Toc186212435)

[第三節 資訊服務供應商存取權限 14](#_Toc186212436)

[第四節 服務變更管理 15](#_Toc186212437)

[第五節 資訊服務供應商定期審查 15](#_Toc186212438)

[第六節 證券商與資訊服務供應商終止、解除、結束資訊委外關係 15](#_Toc186212439)

[第七節 委外第三方或其下包商人員派駐管理 16](#_Toc186212440)

[第八節 專案管理 16](#_Toc186212441)

[第九節 驗收標準 17](#_Toc186212442)

[第十節 服務終止與解除 17](#_Toc186212443)

[第七章 輸出文件記錄 18](#_Toc186212444)

# 目的

為使資訊服務供應商明確遵行本公司供應商遴選、管理、終止與解除等各階段之風險管理之作業流程，落實資訊安全規範要求與控管檢核機制，確保本公司之資訊資產之機密、完整、可用性在委外作業流程得完善保護，特訂定本作業程序。

# 適用範圍

由本公司非屬委託他人作業類之委外資訊服務專案皆屬之，包含提供與系統軟體或硬體有關之服務形態，如電腦軟體與硬體相關服務與人力及技術等整體性之資訊服務、整體規劃、系統整合、系統稽核、軟體開發、軟體維護、軟體採購、顧問諮詢、機房設施管理、備援服務、網路服務、資料庫建置、硬體維護、硬體採購、資料處理以及其他適合辦理委外服務之資訊作業項目均適用。

# 名詞定義

### 資訊委外：係指證券商將部分或全部之資通服務由組織外之軟硬體供應與維運商、跨機構合作夥伴提供。

### 資訊資產：係指與資訊處理相關之資產，包括硬體、軟體、資料、文件及人員等。

### 資通系統：係指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

### 資通服務：係指與資訊之蒐集、控制、傳輸、儲存、刪除、其他處理、使用或分享相關之服務。

### 資訊服務：係指提供與系統軟體或硬體有關之服務形態，包含系統發展類、維運管理類及雲端服務類。

### 雲端運算服務：透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務。

### 營業秘密：係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷 售或經營之資訊，而符合下列要件者：

(一) 非一般涉及該類資訊之人所知者。

(二) 因其秘密性而具有實際或潛在之經濟價值者。

(三) 所有人已採取合理之保密措施者。

### 存取：係指存取資訊資產的各種方式，包含取得、使用、保管、查詢、修改、調整、銷毀等。

### 專案負責人：係指專案經理或該項業務權責部門主管或其指派之人員。

### 資通安全機制 (Security by design)：係指服務與產品規劃設計時即融入資通安全的概念，於開發流程中的設計階段，列出安計時即融入資通安全的概念，於開發流程中的設計階段，列出安全需求、辨識安全風險及套用控制措施，以作為後續安全功能驗全需求、辨識安全風險及套用控制措施，以作為後續安全功能驗證的基礎，落實安全的軟體生命週期。證的基礎，落實安全的軟體生命週期。

### 隱私保護機制隱私保護機制 (Privacy by design)(Privacy by design)：係指服務與產品規劃設：係指服務與產品規劃設計時即融入隱私保護機制的概念，於開發流程中的設計階段，計時即融入隱私保護機制的概念，於開發流程中的設計階段，列出隱私保護需求、辨識相關風險及套用控制措施，以作為後列出隱私保護需求、辨識相關風險及套用控制措施，以作為後續安全功能驗證的基礎。續安全功能驗證的基礎。

### 資通安全事件：係指系統、服務或網路狀態經鑑別而顯示可能資通安全事件：係指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。統機能運作，構成資通安全政策之威脅。。

# 相關文件

### SO-02-001\_委外駐點人員作業程序。

### SO-02-001-F01\_委外（第三方）作業人員保密承諾書。

### SO-02-001-F02\_委外（第三方）作業人員進駐之工作規範。

### SO-02-001-F03\_資訊安全政策聲明。

### SO-03-001-F02\_臨時服務證申請單。

### 委託他人作業準則。

### 委託他人作業準則-作業委外廠商定期審查表

# 權責

## 委外第三方

### 如有駐點人員或因工作需要存取本公司資訊資產之需求，應瞭解並遵照本公司所有相關安全規範。

### 存取本公司所屬之資訊資產，應簽訂保密合約，承諾保護之責任，違反安全規範時，願意接受合約相關罰則。

### 進行專案時，依據專案工作規劃之各項要點進行。

### 委外第三方如有處理本公司機密資料或文件，應遵循本公司例行查核項目，並接受本公司定期查核。

## 供應商管理流程負責人

### 負責設計供應商管理流程之關鍵績效衡量指標（KPIs）。

### 負責供應商管理流程管理報表及績效管理指標之檢視及報告。

### 負責追蹤與檢討各供應商服務審查結果及改善計畫。

### 負責提出供應商管理流程運作之改善建議。

## 供應商管理主管

### 確保各合約符合現行相關管理體系之要求。

### 協助合約內容管理，確保合約能支援本部與達成本公司服務之可用性標準。

### 提交服務水準報告，交由證券商審核備查。

### 負責製定及啟動年度供應商審查及其標準，供應商審查表內容需包含(1)供應商提交服務水準報告達成情形，(2)供應商資訊安全狀況評估。

### 審查結果認為有稽核之必要時，得對資訊服務供應商進行稽核。

## 本公司專案負責人及專案負責單位

### 為與各供應商聯繫、溝通之窗口人員。

### 於評選供應商及簽訂合約協議前，專案負責人應明確告知委外第三方有關本公司之相關資訊安全規範之要求；如需提供委外第三方本公司相關資訊，應與第三方簽訂保密合約後方能提供。

### 與委外第三方簽訂合約時應使用本公司所規範委外服務之標準合約，合約應載明驗收標準與程序以及應繳付之文件或產出資料項目，任何修改需經本公司法務人員同意。

### 委外第三方之各項請款，應檢查已符合驗收條件之要求，始得驗收。

### 各項專案工作規劃，應包含各階段之工作項目與內容、工作時程以及控制項目，專案負責人應依時程檢核控制項目。

### 負責合約擬定過程之作業，並監督服務交付與合約執行之情況。

### 配合供應商管理主管執行年度供應商審查。

### 負責供應商改善方案之定期追蹤與報告。

### 提出供應商績效報告與改善建議。

### 掌握管理範圍下之供應商、合約資訊。

### 留存驗收表等相關紀錄。

## 法令遵循暨法務室

於合約簽訂前覆核合約內容的修改。

## 資訊安全人員

### 查核委外第三方存取本公司資料之相關紀錄。

### 查核合約內容資訊安全相關條件是否符合。

### 查核簽訂合約前，是否填寫《SO-02-002-F11\_資訊服務供應商資安注意事項遴選檢核表》。

## 資訊部主管

### 核准《SO-02-002-F11\_資訊服務供應商資安注意事項遴選檢核表》。

### 對於第三方違反之相關安全規範，討論、改善、追蹤處理情形及懲處決定。

# 作業內容

## 資訊服務供應商遴選

1. 合約金額100萬(含)以上之案件，應評估資訊委外業務項目之資通安全可行性及資訊服務供應商作業能力，確保業務項目委外處理之品質。專案負責人應填寫《SO-02-002-F11\_資訊服務供應商遴選原則檢核表資訊服務供應商資安注意事項遴選檢核表》並經資訊部主管核准。
2. 資訊服務供應商資安注意事項遴選原則

#### 採購管理單位應評估資訊服務供應商之維運能力，如財務能力、專業能力及經驗實績等。

#### 委外單位應評估資訊服務供應商是否具備完備之資通安全管理措施或通過第三方驗證。

#### 委外單位應視專案性質，評估是否將資通安全要求列入成本估算，如：安全性檢測行動應用程式資安檢測、源碼檢測、弱點掃描等。

#### 委外單位應評估資訊服務供應商是否具備足夠資安能量，倘有集中度過高疑慮（與本公司簽訂委外作業合約3份以上，或服務金融同業3家以上）應由相關資訊單位共同執行風險評估，評估結果應提報適當管理層級並取得同意。

#### 如為雲端運算服務供應商，應評估其是否具備完善之雲端運算資通安全管理措施或通過第三方驗證。

1. 一年內再次對資訊服務供應商作相同設備採購，未涉及任何維運或專案服務，則視同供應商服務內容未變更，採購時不需再執行供應商遴選表風險評估。如為作業委外專案，則另依據《委託他人作業準則》辦理。

## 資訊服務供應商合約

### 合約簽署前之準備規範

#### 專案負責人於評選供應商初期，在提出「建議書徵求文件」（RFP, Request for Proposal）時，應事先以書面方式告知委外第三方本公司資訊安全相關要求，並納入合約應遵守之規定及驗收條款中。

#### 資訊服務供應商提供之建議書應包含下列項目

##### 證券商採購需求產品及服務。

##### 資訊服務供應商應符合之資安要求 例如：證券商資安政策、券商公會資通系統安全防護基準自律規範 。

##### 資訊服務供應商之專案管理能力 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 。

#### 簽訂合約應依委託業務性質提供本公司委外服務與開發使用合約書之標準範本，如有修改標準合約需求，需經法令遵循暨法務室覆核與同意，合約審核作業流程請參考《SO-02-002-附件A\_合約審核作業流程圖》：

##### SO-02-002-F06\_系統委外開發合約書範本。

##### SO-02-002-F07\_維護合約書範本。

##### SO-02-002-F08\_設備採購暨系統整合服務合約書範本。

##### SO-02-002-F13\_勞務採購契約書範本。

##### SO-02-002-F14\_軟體維護合約書範本。

#### 合約內容應涵蓋委外第三方下包商之規範，如委外第三方有下包商情形，其有義務提供下包商之背景資料予本公司，並負起監督下包商遵守本公司安全規範之責任，合約亦需註明下包商等同委外第三方之規定以及違反相關規範之責任歸屬與罰則。

#### 選商過程中如存在資訊資產交換，應備妥保密協議書，並於交換與採購產品或服務相關之機敏性資訊前要求供應商簽署。

#### 委外合約申請用印時，需附上《CIS內部簽核表：作業委外核定-資訊服務供應商類》之核可簽文。

### 證券商與資訊服務供應商之合約

#### 證券商與資訊服務供應商之合約內容應依服務範圍的不同，宜包含下列各項：

#### 基本要求

##### 合約期限。

##### 服務範圍。

##### 服務交付日期。

##### 服務水準要求（一年期(含)以上合約，合約服務水準條款應包含客服支援時段、問題支援方案、每月可歸責於廠商之D級事件之件數上限及超出件數之補償條款，如延長保護；並得視委外情境調整服務水準指標）

##### 服務變更規範。

##### 服務驗收之標準。

##### 資通安全事件通報及應變處理作業程序。

##### 對資訊服務供應商之稽核權條款。

##### 合約轉讓或同意分包之規範。

##### 保密義務條款。

##### 罰則與損害賠償條款。

##### 爭議處理程序。

##### 違約處理條款。

##### 合約終止規範。

##### 合約終止後之處理。

##### 保固。

##### 權利及責任。

#### 委外作業如涉及資訊委外服務或產品，合約應載明事項：

##### 載明資訊委外服務或產品之智慧財產權及其授權範圍。

##### 資訊服務供應商如分包予其他供應商應載明(異動亦同)。

##### 第一類證券商應載明採購之服務與產品於規劃設計時納入服務與產品之機敏資料保護、授權與認證、安全性更新等。

##### 第一類證券商應載明採購之服務與產品於規劃設計時納入隱私保護機制 (Privacy by design) 之要求。

#### 資訊服務供應商之資安應符合下列要求：

##### 資訊服務供應商之法令遵循義務

###### 資訊服務供應商應遵循之本公司資安要求事項，以及其他相關法規遵循與保密義務，如個人資料保護法。

###### 如涉及資通系統開發、維護與監控，資訊服務供應商應遵循「中華民國證券商同業公會資通系統安全防護基準自律規範」。

###### 如涉及使用雲端運算服務，資訊服務供應商應遵循「中華民國證券商同業公會新興科技資通安全自律規範」。

##### 資訊服務供應商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。

##### 資訊服務供應商揭露第三方程式元件之來源與授權證明。

##### 資訊服務供應商處理證券商委託服務各項範圍資訊，能於證券商要求期限內提供。

##### 資通(訊)服務供應商於處理證券商資料應有明確區隔，並應予以加密保護。

##### 證券商應載明要求資訊服務供應商於知悉存有任何潛在問題和危害(如：於其他客戶端發生重大系統異常) ，且其可能影響受託業務時，立即通知證券商並採取相關補救措施。

##### 證券商電子交易之即時報價，如採用不同資訊服務供應商互為備援外，與資訊服務供應商之契約，應要求提供備援主機與備援系統相關證明文件，每年應與證券商進行一次主備援切換測試演練並保存相關演練記錄文件。

##### 第一類證券商之資訊服務供應商應提供取得之資安及品質證照。

### 應於簽約程序中確認資訊服務供應商保密切結事宜。

### 資訊服務供應商發生資安事件致本公司受到影響時，資訊服務供應商的處置程序及責任。

### 應簽署相關文件

#### 《SO-02-001-F01\_委外（第三方）作業人員保密承諾書》。

#### 《SO-02-001-F03\_資訊安全政策聲明》。

#### 《PIMS-P-01-F01\_個人資料保護政策聲明》。

## 資訊服務供應商存取權限

### 專案負責人應向資訊服務供應商告知組織之資訊安全相關規範，為保護本公司資訊資產，資訊服務供應商經申請獲本公司同意後，始有存取合約專案相關資訊資產權限。

### 本公司應對資訊服務供應商人員電腦通行使用權利進行適當控管，並應於委外合約期間結束後立即收回該項權利。

### 資訊服務供應商之保護責任：

#### 資訊服務供應商對於資訊之存取控制措施不得低於與本公司協議之規定及「營業秘密法」第七條第一項及第二項。

#### 資訊服務供應商應保證該資訊資產、營業秘密之使用，僅限於原申請範圍。

### 證券商應管理並至少每半年一次檢視資訊服務供應商之駐點作業、實體與邏輯存取權限，包含作業地點的配置、網路設備及主機連線、電腦的使用、電腦機房的進出、門禁臨時卡的申請等。

## 服務變更管理

### 資訊服務供應商服務內容如需變更，本公司之專案負責人應重新對資訊服務供應商變更之服務內容進行風險評估。

### 修改合約條文需經法令遵循暨法務室覆核與同意。

## 資訊服務供應商定期審查

### 一年(含)以上、且合約金額達100萬(含)以上之案件，應定期進行資訊服務供應商定期審查作業，確認服務水準等資安應配合事項達成情形，執行作法如下：

#### 如為延續案件，應定期每年度第四季執行定期審查作業，或於簽新約時舊去年執行情形進行定期審查作業。

#### 如為首次起案之新案，應於每年度第四季結束前完成定期審查作業。

#### 如就定期審查結果認為有稽核之必要時，本公司得自行或授權第三方得對資訊服務供應商進行稽核

#### 資訊服務供應商定期審查作業應留存簽核紀錄，應於《cis內部簽核表：作業委外定期審查-資訊服務供應商類》附上《委託他人作業準則》之《作業委外廠商定期審查表》並經單位主管核准。

## 證券商與資訊服務供應商終止、解除、結束資訊委外關係

### 證券商與資訊服務供應商之資訊委外關係於終止、解除或結束後，證券商應立即停止資訊服務供應商所涉及之實體與邏輯存取權限，並回收或請資訊服務供應商銷毀屬於組織之資訊資產、營業秘密，必要時可要求資訊服務供應商出具銷毀證明，另要求：

#### 本公司若決定將產品或服務由原資訊服務供應商移轉回證券商或至其他資訊服務供應商時，原資訊服務供應商與證券商 雙方應遵循之資安要求事項。

#### 資訊服務供應商於資訊委外關係所涉及本公司之資訊資產，應於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務供應商。

#### 本公司與資訊服務供應商之資訊委外關係於終止、解除或結束後，資訊服務供應商應持續遵守保密承諾。

#### 終止程序執行之時限。

## 委外第三方或其下包商人員派駐管理

委外第三方或下包商派駐人員，應遵守下列安全規定：

### 派駐人員派駐時間超過七日以上，本公司專案負責人填寫《SO-03-001-F02\_臨時服務證申請單》，申請表應詳列人員名單，如非固定人員，應列出可能派駐人員名單、申請的數量、進入工作場所、派駐起迄時間，依程序向人事單位申請，派駐時間如有延長專案負責人應重新填寫單申請。

### 專案負責人應告知供應商派駐人員應遵守本公司資訊安全相關規範與罰則，派駐人員(駐點時間超過三個月)或委外第三方應簽立以下，派駐人員進出工作場所應配帶識別證於明顯位置。

#### 《SO-02-001-F01\_委外（第三方）作業人員保密承諾書》。

#### 《SO-02-001-F02\_委外（第三方）作業人員進駐之工作規範》。

#### 《SO-02-001-F03\_資訊安全政策聲明》。

#### 《PIMS-P-01-F01\_個人資料保護政策聲明》。

### 派駐人員因工作需要使用本公司資源時，應依相關規定程序，填寫CIS \_需求申請單，申請表應詳列使用之設備、IP位址與網域連結…等，經擁有者授權後開放。

### 派駐人員使用之電腦設備，應遵守本公司防毒管理作業規定，交付本公司檢驗後方可連接至本公司內部網段。

## 專案管理

### 本公司專案負責人於專案與第三方確認事項，包含：

#### 專案組織成員之角色與職責。

#### 確認第三方於專案進行中，專案預計之時程進度及檢查時點。

#### 對於專案進行中之各項議題，擬定解決及後續追蹤之程序。

#### 安全事故或緊急事件之通報程序。

#### 雙方對於專案中應產出項目或交付的文件格式及內容概要。

#### 軟硬體變更管理程序。

#### 預計產出項目之驗收標準。

### 專案中之異動資料、專案情形及項議題應留記錄，以供查核。

### 每年至少於12月前，供應商管理主管應針對當年度有履約且金額為100萬元以上採購供應商進行供應啓動供應商審查。若審查結果未達標準，專案負責人須對該供應商於審查表填寫審查結論，並造蹤與檢討供應商改善計畫。供應商管理主管並視審查結果評估是否要進行供應商稽核作業。

## 驗收標準

### 驗收要求與標準

系統委外開發驗收標準應提供之文件可包含：

#### 安裝程序、變更、編譯，過版程序、復原程序，作業手冊與操作手冊。

#### 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（四）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。

### 驗收流程與程序

委外第三方之各項請款，應檢查已符合驗收條件之要求，需配合總務室驗收流程進行驗收，如分次驗收應於該表上註明分次驗收之第幾階段，由資訊安全人員確認符合委外作業安全規範後，始得付驗收。

## 服務終止與解除

一、於專案終止、解除或結束後，應立即停止資訊服務供應商所涉及之實體與邏輯存取權限，並回收或請資訊服務供應商銷毀屬於組織之資訊資產、營業秘密，必要時可要求資訊服務供應商出具銷毀證明。

二、終止執行之服務持續性要求事項，其應包含下列各項：

（一）若產品或服務由原資訊服務供應商移轉回組織或至其他資訊服務供應商時，原資訊服務供應商與組織雙方應遵循於合約中要求之資安要求事項。

（二）明列使用於資訊委外專案中所涉及組織擁有之資訊資產，以利於專案終止時得以完整歸還於組織、確保銷毀或轉交予其他資訊服務供應商。

（三）承上，明列歸還、轉交或銷毀之程序，必要時可要求提供證明文件。

（四）當資訊委外關係終止後，保密承諾應如同合約所述，保持其持續性。

# 輸出文件記錄

### SO-02-002-附件A\_資訊服務供應商作業程序圖。

### SO-02-002-F01\_委外開發驗收表。

### SO-02-002-F06\_系統委外開發合約書範本。

### SO-02-002-F07\_維護合約書範本。

### SO-02-002-F08\_設備採購暨系統整合服務合約書範本。

### SO-02-002-F09\_合約檢核清單。

### SO-02-002-F10\_供應商支援紀錄表。

### SO-02-002-F11\_資訊服務供應商資安注意事項遴選檢核表。

### SO-02-002-F12\_設備採購合約書範本。

### SO-02-002-F13\_勞務採購契約書範本。

### SO-02-002-F14\_軟體維護合約書範本。