

## 附件六、保險業核心資訊系統作業委外資安注意事項

### 一、本注意事項目的

為協助保險業於辦理核心資訊系統作業委外過程，於各階段(包括「計畫作業」、「招標」、「決標」、「履約管理」、「驗收」及「保固作業」等)考量相關資訊安全需求，以適當管理供應鏈風險，提升相關系統作業委外安全，特訂定本注意事項。

保險業宜參照本注意事項辦理。

### 二、計畫作業階段

#### (一)核心資訊系統作業委外可行性分析：

1. 篩選適合委託辦理之業務項目，確定該項業務委外之資訊安全可行性。
2. 將資安列入成本估算項目，進行效益分析。
3. 評估資訊系統作業委外資安風險與對策。

#### (二)核心資訊系統作業委外開發案，專案成員中應有資安人員參與。

#### (三)識別核心資訊系統作業委外資安需求：

1. 委外業務涉及敏感性或含資安疑慮時，應識別委外廠商之限制。
2. 宜邀請廠商提出資安對應措施方案。

### 三、招標作業階段

#### (一)招標文件之制定與發布包含以下項目：

1. 採購產品或服務之資安要求事項。
2. 明定資安要求事項之服務水準(如：系統可用率、安全管控機制、稽核作業、資安檢測與弱點修補之責任與義務等)。
3. 未符合資安要求事項或服務水準時，應訂定罰責標準，依損害程度向委外廠商進行求償或罰款。

#### (二)準備保密協議書。

#### (三)委外廠商遴選準則之定義與實作：

1. 委外廠商之資安能量，評估核心系統是否承接過多會員公司之專案及其因應措施。
2. 要求委外廠商允許經授權之第三方稽核，以確認所定義資安要求事項之遵循性。
3. 委外廠商對其提供產品或服務之資安管理機制。

#### (四)評估委外位置與提供產品或服務之位置，對資安是否有不利影響，並納入評估項目。

#### 四、決標作業階段

與委外廠商簽訂合約或協議時，遵循相關安全管理措施，其內容包含：

- (一)應訂定相關資訊安全管理責任，載明與委外廠商雙方之資安角色與責任，若有分包，需一併確認分包計畫可能產生之資安風險。
- (二)資訊安全事件之通報流程及處理程序。
- (三)委外廠商履行合約或協議時所提供軟體(或交付標的物)為交付產品，需具備合法性且不得違反智慧財產權之規定或侵害第三人合法權益，確認軟體(含元件)之使用版權及安全性。
- (四)委外廠商進行資訊系統開發或維運時，若涉及客戶、員工個人資料，需考量具個人資料安全防範措施。
- (五)委外廠商提供之優規產品或服務，仍需確認可能產生之資安風險。

#### 五、履約管理階段

- (一)建立委外廠商管理規範，其內容應含委外廠商之人員管控，雙方皆應指定專案負責人，負責督導及辦理各項資安要求事項。
- (二)持續識別資訊系統作業委外風險，並採取適當管控措施。
- (三)監督廠商於人員、實體環境及委外管理等資安要求事項是否落實執行，並建立適當檢驗機制，以確保管理機制有效落實。
- (四)委外廠商對相關作業人員進行資訊安全教育訓練，使其充分了解資安政策及責任。

#### 六、驗收作業階段

委外作業於驗收程序，注意事項如下：

- (一)顧問訓練類:確認使用檢測工具的安全性和教育訓練時安裝軟體的安全性。
  - (二)系統發展類：
    - 1. 要求委外廠商揭露第三方程式元件之來源與授權。
    - 2. 要求委外廠商提供資訊系統之安全性檢測證明，如：源碼檢測、弱點掃描或滲透測試等。
  - (三)維運管理類：每半年執行系統弱點掃描。
  - (四)雲端服務類：確認雲端服務供應商宣稱之資安認證範圍(含功能)。
- 委外關係終止或結束時，應依本自律規範第十六條第一項之規定辦理。

#### 七、保固作業階段

- (一)保固服務：系統異常造成運作中斷或部分無法正常運作時，如可歸責於廠商時，廠商應依契約規定，履行保固服務或進行異常管理。
- (二)異常管理：系統若有重大資安問題，應有變更計畫，評估潛在資安衝

擊及提供變更及復原程序。

#### 八、其他應注意事項

- (一)於籌獲套裝軟體時，應確認可能產生之資安風險。
- (二)資訊系統作業委外服務案中，委外廠商有須結合第三方服務提供者 (Third-party Service Provider, TSP) 方能提供完整服務之情形，應將 TSP 可能產生之資安風險納入評估。