Sunfun

尚凡國際創新科技股份有限公司

資訊安全管理規範

2025.03.07修訂

目　次

資訊安全管理規範

壹、資訊安全政策

公司之資訊安全政策訂定目的在於確保營運及服務提供流程中之資訊機密性、完整性及可用性。所有人員需依循此資訊安全政策進行營運及服務之資訊管理。

一、客戶權益政策

所有資訊處理及營運管理均需以客戶權益為優先，任何影響客戶權益之資訊處理過程或方式，均應被檢討並依影響客戶權益最小的方式為之。

二、遵循法令政策

(一) 所有不合於法律、法規、命令或目的事業主管機關相關規定之資訊處理，一律禁止。人員發現有違反法令之虞的資訊處理，應向相關主管進行回報。須遵循之法律包括個人資料保護法、商標法、消費者保護法及其他與電子商務交易相關之法令。

(二) 應尊重智慧財產權，避免使用未經授權之電腦程式、違法傳送受著作權法保護之著作，及其他可能涉及侵害智慧財產權之行為。

三、電子商務交易保護政策

(一) 於電子商務交易過程中，應確保所有交易資訊的機密性、完整性及其可用性。

(二) 所有交易過程需確保交易的不可否認性，相關交易紀錄依法律要求之保存期

限進行保存，備份及其他資保全之安全措施應被執行以確保交易資訊之可用性。

(三) 所有提供客戶之產品資訊、價格資訊及其他交易重要資訊均須確保其正確性。

四、 個人資料及隱私保護政策

所有交易資訊涉及個人資料均須按個資法之要求，依法進行對於當事人進行告知、取得同意及限制僅使用合於特定目的之利用。本公司嚴禁一切非法之蒐集、處理、利用個人資料。本公司不使用任何有非法取得，或未確認合法性之個人資料。

五、 設備及資源使用政策

本公司所有提供之設備包括網站主機、個人電腦、資訊處理設備、通信設備、網路設備及其相關資源或資料僅允許作為公司營運相關目的使用，本公司禁止人員將公司設備及資源使用於任何個人目的或非公司營運目的之使用。

六、 機密資料保護政策

(一) 本公司明訂公司營運資訊與所有客戶交易相關資訊均為本公司所定義之機密資訊，所有人員需恪遵保密之義務，於資訊處理過程中實施合適之保密控管機制。對於有洩漏機密之虞的資訊處理，應立即回報相關主管。

(二) 本公司所有人員、委外廠商或與資訊處理相關之第三方均應簽署保密協議書，並遵循相關保密義務及規定。

七、 網站安全維護政策

網站為本公司營運之主要機制，網站所使用之網路資源、主機、資料庫及其處理之營運及交易資訊均需施予合適的安全維護。人員發現有網站的安全漏洞或有違反資訊安全政策的可能事件應主動向相關主管回報，並積極協助維護網站之安全。

八、資訊安全風險評估與風險處理

為了確保本公司交易資訊安全，所有資訊處理設施及相關資訊資產及服務均須進行風險評鑑，並針對風險評鑑之結果進行風險處理。重要資訊資產及服務於上線前應完成風險的評鑑。

九、委外管理政策

本公司委外管理電子商務相關業務應進行委外之控管。其中包括：

(一) 應訂定委外合約，委外合約中須明定資訊安全相關要求。

(二) 應定期檢視委外廠商提供之服務內容是否符合合約之規範。

(三) 委外服務內容包括交易資訊及消費者個人資料之處理，應與委外廠商簽訂保密協議。

十、重要資訊安全控管措施

(一) 主管應確認新進人員、合約商及第三方人員於接觸公司相關營運、交易資訊前熟知公司之資訊安全政策。每年應於政策更新後重新對人員進行宣導，並要求人員遵循本政策。

(二) 定期檢討本資訊安全政政策，並於電子商務環境發生變動時進行檢討及更新。

(三) 應定期或於電子商務環境發生重大變化時，識別電子商務服務所面臨的威脅及弱點，並考量適切的管控。其中包括資產盤點、風險評鑑與產生風險處理

計畫或建議。

(四) 應定期執行電子商務相關營運系統之帳號及權限審查。

(五) 應定期對公司人員執行資訊安全認知教育訓練，內容應至少包資訊安全政策宣導、電子商務資訊安全相關知識、安全責任及相關法規命令之宣導等項目。

(六) 應定期對公司電子商務相關網站進行弱點的識別，並採取適當措施強化。

(七) 重要交易資料應定期備份，重要系統應建立備援機制。

(八) 定期內部稽核，且留存紀錄並提出矯正預防措施。

貳、人員及組織安全

一、人員安全

(一) 人員能力、認知與教育訓練

1.新進人員應於開始接觸公司營運及交易資訊前完成資訊安全教育訓練，包括資訊安全政策、安全責任、相關法規命令之認知訓練。

2.公司應定期資訊安全訓練課程，其中包括資訊安全政策宣導、電子商務資訊安全相關知識、安全責任及相關法規命令之宣導。

3.公司應定期檢討重要資訊安全管理人員之能力是否需要接受專業之資安課程，或重要資安設備之操作技能訓練，以強化資訊安全之管理能力。

(二) 人員資訊安全管理責任

1.一般人員之資訊安全管理責任

(1)公司人員均需遵循「CC-100 資訊循環」內部控制制度之規定。

(2)公司人員有義務妥善保管其郵件信箱之帳號與密碼，並遵守公司密碼相關規定。帳號擁有者應為此組帳號密碼登入系統後所進行之一切活動負責。

(3)為維護公司人員自身權益，請勿將帳號與密碼洩露或提供予第三人知悉，或出借或轉讓他人使用。

(4)公司人員應加強對電子郵件使用安全之認知，避免開啟來路不明的電子郵件。

(5)遵循公司之機密性資訊管理政策，對於所有營運及客戶交易資訊進行保護。

(6)所有人員均應簽署員工保密協定(如【附件 1】)，並遵循保密之義務。

2. 資訊安全管理人員責任

為確保資訊安全管理之推動，公司之資訊管理責任分配時，應確保以下責任均被指定負責人員：

人員	工作項目
總經理	• 政策、目標之研擬與督導 • 各項資源之分配、協調與督導 • 交辦及督導各項行政事務 • 協調整合內部資訊安全管理工作 • 核准個人資料之蒐集、處理、利用事宜
網管部主管	• 網站及伺服器硬體之安全管理 • 定期審查各主機之安全 log • 定期審查防火牆 log • 網路安全管控 • 資料庫安全 • 客戶個人資料保護
程式部主管	• 網站系統軟體、程式碼之檢查 • 網站系統之變更管理
客服部主管	• 資訊安全事故通報窗口
產品部主管	• 客戶個人資料保護企劃擬定及推行
人事部主管	• 員工個人資料保護
內部稽核主管	• 內部稽核

(1)網路安全： 網路設備及網路資源管理。

(2)系統安全： 包括網站軟體硬體、電子商務相關機制主機等。

(3)人員安全及教育訓練： 人員聘僱及安全管理、人員認知、教育訓練。

(4)委外內容管理： 包括合約及定期稽核、檢視服務結果或要求定期報告等

事項：

(5)內部稽核： 定期執行內部管理規範及個人資料保護執行狀況之稽核作業。

本管理責任分配表應定期檢討更新，或於職務、管理責任變動時更新，並通知相關人員。

(三) 人員聘僱及離職管理

1.公司聘僱新人，應考量該職位之資訊安全能力需求並審查人員之能力與需求是否符合，必要時應進行相關背景查驗。

2.公司聘僱新人，應協助並確認人員了解其資訊安全責任及管理責任，以降低發生偷竊、舞弊及資訊資產誤用的風險。

3.人員離職、調整職務或調職時應指派交接人員，並容許足夠的交接時間。

4.離職員工應返還公司資產，包括軟、硬體設備及相關資訊資產。

5.員工離職後，應立即刪除其系統之存取權限。

二、實體及環境安全

(一) 辦公場所及電腦設備存放場所安全管理

1.辦公場所及電腦設備存放場所應實施門禁管控，以防止未授權的存取或破壞。

2.重要設備或實體資訊存放地點應予以保護，確保重要之資訊資產不受到火災、洪水、地震、爆炸、或其它天然或人為災難的損害。

(二) 人員及設備進出管制

1.辦公場所及電腦設備存放場所應有進出管制紀錄。

2.重要資訊資產攜出入辦公場所或電腦設備存放場所應有適當之核准過程及留存紀錄。

(三) 資訊資產及個資盤點

1.公司每年應進行一次資訊資產盤點，並產出資產清冊，或於重要資訊資產異動後更新資訊資產清冊。

2.資訊資產應設定保管人員。

3.公司每年應進行一次個人資料盤點，並產出個人資料資產清冊。

三、個人電腦、資訊處理設備安全維護

(一) 個人電腦、資訊處理設備之管理

1.防毒軟體：所有處理電子商務相關之個人電腦均應安裝防毒軟體，並定期或設定自動更新病毒碼。

2.個人電腦須設定螢幕保護程式，於 10 分鐘未使用該電腦後自動上鎖並以通行碼(Password)保護，以防止電腦遭未授權使用。

3.電腦或其他資訊處理設備應設定自動或定期更新最新的系統補強(Patch) 以防止系統之漏洞或弱點所造成之威脅。

(二) 個人電腦、資訊處裡設備中之資訊保護

1.個人電腦、資訊處裡設備中，如因業務需求存放機密資訊，應給予適當的保護例如加密、或設定存取權限以避免遭未授權之存取。

2.機密資訊不應置放於網路公開之分享區。以電子郵件或其他電子傳訊方式進行資訊之傳送時，應予以加密或以密碼保護後傳送。

3.個人電腦存放重要資訊者應定期進行資訊備份，備份後的媒體或檔案應注意其安全防護，以確保資訊之可用性及防止未授權存取。

4.個人使用可攜式媒體(例如外接式硬碟機、USB 隨身碟)進行資料傳送或複製，應有適當之安全防護機制，以確保不被惡意程式入侵或遭到資料的竊取，外來 USB 使用前應進行病毒掃描。

四、網站/伺服器安全維護

(一) 本公司使用之網站、伺服器應安裝防毒軟體及相關防止惡意程式攻擊之安全控管機制，並設定定期或自動更新病毒碼。

(二) 應設定定期或自動更新補強(Patch) ，以避免因系統漏洞或弱點所產生之風險。

(三) 本公司使用之網站應建立網站應用程式防火牆(Web Application Firewall) 以阻絕針對網站應用程式的惡意攻擊。

(四) 應建立網站安全監控機制以確保電子商務網站之安全狀況，並於遭受攻擊或疑似遭受攻擊時進行通報。

五、第三方管理

(一) 如第三方之服務供應商使用或存取公司之營運或交易資訊時，應與第三方服務供應商訂定委託協議(如【附件 4】委外處理個資合約範例)，以確保第三方服務供應商均遵循公司之資訊安全要求。

(二) 涉及個人資料委外蒐集、處理、利用者應依照【附件 4】委外處理個資合約範例進行委外合約的簽訂，以確保合於新版個資法之要求。

(三) 應要求第三方人員於接觸存取公司營運或交易資訊前簽訂保密承諾書(如【附件 2】委外廠商保密承諾書及【附件 3】委外廠商員工保密承諾書)。

參、內容安全

一、 存取控制安全

(一) 公司之重要電子商務系統，包括作業系統及應用系統之應進行使用者帳號管制。人員申請帳號應填寫「應用系統權限新增／取消申請表」，並經由單位主管及處理部門主管核核准後始得使用。

(二) 重要電子商務系統帳號、通行碼<Password>規定最小長度為 8 碼，應定期於 180 天內更換密碼，密碼最短使用天數應為 7 天。

(三) 重要電子商務系統應件立權限管控，並依照不同人員、角色進行權限之配置以確保資訊之存取均符合公司之管理政策。

(四) 對於重要的電子商務網頁及交易資訊必須確保其正確性並進行正確行查核。

(五) 公司重要系統涉及共用者號管理者，應依照本公司「帳號共用管理程序」之規定辦理。

(六) 每年應至少進行一次帳號權限清查，以防止未授權之帳號及錯誤之權限設定。

二、資料、文件、資料庫安全

機密分級及標示

(一) 公司營運及客戶交易相關資訊、客戶個人資料均為機密等級，所有機密等級之資訊均應遵守以下處理規定：

1. 機密等級資訊未經公司授權核可，人員不得向外透漏或傳輸。
2. 機密等級資訊如為紙本形式，應視需求進行機密等級標示，以確保資訊不被誤用或遭未授權存取。
3. 機密等級資訊應避免存放於網路的公共區域。
4. 機密等級資訊如需以電子郵件或其他電子傳訊方式傳輸應予以適當之保護(例如加密或以通行碼<Password>保護後傳輸)。

(二) 重要電子商務網站交易資訊應實施加密機制或其他防止資訊洩漏之機制，以防止重要交易資料遭洩漏、竄改或竊取。

三、儲存/備份安全

重要電子商務交易資訊應依業務需求進行定期備份。

四、資料傳輸安全

(一) 重要電子商務資料與其他外部組織交換時應簽訂交換協議書。(如【附件 5】資料交換協議書)。

(二) 人員於進行資料交換前應建立資料交換申請單取得主管之核准後始得為之。(如【附件 6】資料交換申請單)

(三) 資料交換如採用實體媒體交換時，應進行媒體運送、接收之管制，以利事後

追蹤。

五、個人資料保護安全

(一) 業務單位定期檢討作業及交易流程，以確保個人資料之各項管理作業及個資的蒐集、處理、利用均符合個資法之要求。

(二) 應依照個人資料保護法之規定對於消費者進行資料蒐集前之告知及隱私保護聲明。(如【附件 7】個資蒐集前告知函)

六、證據保全/數位鑑識

(一) 重要之電子商務相關之交易證據、系統日誌、安全事件應定期備份或透過技術機制進行證據之保全以確保證據之有效性。

(二) 相關交易系統及監視機制(如防火牆、錄影設備、門禁系統..) 應定期進行鐘訊同步(校正時間)。

肆、網路安全

一、網路安全

(一) 網路安全管理

1.公司之所有電子商務網站均應建立防火牆及設定合宜之防火牆政策及組態，並定期檢視其組態及政策以防止電子商務交易主機遭受惡意攻擊。

2.公司之辦公作業網路環境應建立防火牆及設定合宜之防火牆政策及組態，並定期檢視其組態及政策以防止辦公作業網路環境遭受惡意攻擊。

3.應建立 IPS、IDS 或 UTM 等機制以阻絕相關惡意攻擊(如 DDOS 等)。

(二) 網路資源及應用管理

1.為確保網路資源不被濫用，公司應建立網路頻寬控制相關機制，以確保所有網路資源之應用均符合公司管理目標。

2.公司應建立人員上網行為監視或網路應用服務監控機制，以確保所有網路使用之行為或應用服務均符合公司管理政策及確保網路資源之可用性。非經許可，公司網路不得使用以下服務

(1) P2P 軟體(如 Foxy、BT 等)。

(2) 線上影片網站或軟體(除因工作需求經特殊授權者外)。

(3) 違反善良風俗之網站或不合法軟體下載網站等。

伍、應用安全

一、程式碼/系統安全

(一) 重要系統程式於上線前應進行原始碼檢測以確保無惡意之程式碼或技術漏洞。

(二) 重要系統上線前應進行變更管理，以確保系統之版本管控、避免變更失敗之風險。

二、郵件安全

(一) 公司之電子郵件帳號需經申請並取得主管核准後使用。

(二) 公司電子郵件帳號使用應僅限於公司業務範圍及公務使用目的。公司得監看公司郵件之內容以確保公司資源不被誤用。

(三) 郵件傳輸公司機密資訊應實施適當之機密保護(如加密或以通行碼<Password>保護)。

(四) 人員應注意不可任意打開來路不明或可疑之信件，應避免點選信件或網頁之不明目的之連結，郵件工具應設定不自動執行程序碼(Script)，以避免遭受惡意之攻擊。

(五) 應定期檢查使用之郵件系統安全及系統紀錄，確保郵件系統不被惡意攻擊。

(六) 應設置垃圾郵件之防護機制，以避免垃圾郵件或其他惡意之攻擊，確保郵件系統的暢通及資源的合理使用。

三、**交易主體及身分識別安全**

(一) 應建立交易主體識別方式，以提供消費者確認公司網站之機制，避免消費者遭惡意網站的詐欺。

(二) 應於電子商務網站建立資訊安全聲明，以確保消費者之權益及對公司網站之信賴。

(三) 應建立消費者識別的方式(例如身分確認機制、郵件確認、簡訊確認等機制)，以避免惡意的消費者詐欺或其他交易糾紛。

四、**交易過程安全**

應建立交易過程安全機制，例如 SSL 安全連線、信用卡安全付款機制，以確保交易過程之安全。

五、**安全評估/弱點掃描/漏洞管理**

(一) 應定期進行網站弱點掃描或其他網站安全評估方式，以確保電子商務網站系統無可被惡意攻擊利用之弱點或系統失能的狀況。

(二) 弱點掃描及安全評估後應進行相關的補強或系統調整。

(三) 應定期進行人員之相關資訊安全知識及政策的宣導或教育訓練。

陸、個人資料管理程序

一、個人資料基本管制程序

(一) 個人資料保存與刪除管理作業

1. 個人資料之保存應注意

A. 查詢相關法律對於資料保存最小年限之要求。

B. 查詢相關法律對於個人資料保存是否設置最長年限。

C. 與告知之蒐集之目的有合理的關聯，並在特定目的消失後主動或依當事人請求進行刪除。

D. 個人資料、軌跡資料及蒐集相關告知及同意證據，如無其他法令限制，建議應至少保存五年，以確保相關證據於個資法損害賠償請求權時效內均能完整提出。

2. 個人資料之存安全

A. 個人資料應依照本規範對於資訊資產之保護邀其進行保護。

B. 個人資料於處理過程中應注意保存其正確性。

3. 個人資料的刪除

A. 當蒐集之特定目的消失後，應主動刪除個資。

B. 公司應依照當事人的請求，進行資料的刪除。

C. 個人資料如因業務需求無法刪除時應符合以下法定的要求其中之一項

a. 有法令規定或契約約定之保存期限。

b. 有理由足認刪除將侵害當事人值得保護之利益。

c. 儲存方式特殊致不能刪除或耗費過鉅始能刪除。

d.其他不能刪除之正當事由。

(二) 個人資料盤點作業

1. 個人資料資產盤點

A. 每年應最少進行一次資料資產盤點作業，清查所有包含個人資料之個人資料檔案包括

a. 紙本資料

b. 各類電子檔案資料(Word, Excel, TXT, XML 及各類的檔案格式中包括系統暫存檔案)

c. 資料庫 (各式資料庫內容)

d. 其他形式 (備份媒體中、網路檔案….)

B. 盤點前應先進行業務流程、資料流程、個人資料流程的流程分析，並注意資料流向，包括流向內部單位、外部單位及第三方單位等資料流程。

C. 盤點時可以輔以使用各類搜尋引擎或搜尋工具進行個資的技術性盤點，對於不同形式、管道之個人資料應助其軌跡及衍生資料的產生。

2. 個人資料行為盤點

A. 個人資料行為規範盤點應併同於個人資料資產盤點時進行盤點或更新。

B. 個人資料行為盤點主要在盤點法律所要求進行之各項應辦事項：

a. 蒐集、處理、利用之行為

b. 蒐集前告知行為 (§ 8, 9)

c. 蒐集、處理之合法要件(§ 19)

d. 利用及特定目的外利用個資之合法要件 (§ 20)

e. 當事權利之行使 (§ 3, 10~14)

C.個人資料行為盤點應包括執行證據之盤點

a. 執行告知之證據

b. 執行各項同意之證據

c. 當事人行使權利後執行的證據

(三)個人資料風險評鑑

A.個人資料適法性風險評鑑主要在透過個人資料行為盤點結果對應法律要求項目的比對，來了解現行作業是否有違法的風險。

B.依照個人資料適法性風險評鑑結果判定為有違法風險之項目，電子商務業者應立即提出改善計畫或進行相關的矯正預防措施以避免違法。

二、個人資料蒐集管理程序

本公司於蒐集個人資料時應遵循以下作業程序

(一) 個人資料蒐集前管控作業

個人資料之蒐集應依法進行，本公司為非公務機關，於蒐集個人資料除遵循法令之要求，並應遵循本規範之政策不得蒐集未經確認為合法來源之個人資料。

1. 蒐集合法性檢查

A.於新個人資料蒐集行為進行前應進行個人資料蒐集告知函【附件 7】。

B.個人資料項目應依照資產管理辦法進行個人資料資產擁有人(Owner)之指派，擁有人依照規定應進行該個資資產之發展、控管及保護事項，其他單位或其他目的須利用本個人資料資產者應取得資產擁有人及管理階層之同意

2. 間接蒐集來源合法性，本規範之政策規定，本公司不得處理或利用未確認合法性之個人資料來源，於間接蒐集個人資料前應特別注意其資料來源之合法性。

(二) 個人資料蒐集監督作業

1. 前端作業監督:

個資因應專案小組應進行前端蒐集作業之監督，確保所有蒐集的作業均符合個人資料保護法之規定。

2. IT 處理作業監督:

蒐集監督作業應延續到個人資料進入個人資料檔案或個人資料管理 IT 系統內為止，個資因應專案小組應於首次蒐集個資作業完成後進行對於個人資料的蒐

集完整性及正確性查核，以確保所有的個人資料蒐集作業均依核准的方式完成蒐集。

3. 後續監督作業，個資因應專案小組應定期進行對於個資蒐集作業及內容正確性的查核，以確保所有作業均在合於規範及合法的狀態下進行。

三、個人資料處理管理作業

本公司於處理個人資料時應遵循以下作業程序

(一) 處理前管控作業

1. 資料處理人員，應確認所處理之資料均符合個人資料蒐集告知函中的資料項目，如果蒐集內容有超出或差異的部分，應主動向前端蒐集人員反映或向管理階層報告，並於改善後進行處理作業。

(二) 個人資料處理作業

1. 處理作業中涉及資料備份者，應於每年度個人資料資產盤點中進行該項資產的盤點。

2. 處理紙本紀錄者，應於資產盤點作業中建立該項目之清冊，並且應依照本規範進行資產的機密等級標示及後續之資訊保護處置，含個人資料之紙本紀錄依規定應屬於機密資料，除應標示機密等級外、進行檢索、編號標示以確保資料之完整性外，應進行實體防護(如上鎖)，以確保該個人資料資之安全。

3. 當公司內部需要進行複製，或傳送個人資料時 (非利用行為)，應向權責主管提出申請，核准人員應判斷該處理作業是否為個資法第二條中所規範之項目，包括為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。凡超出本範圍之需求，應透過【附件 8】個資利用申請書進行利用或特定目的外利用之申請。

(三)　個人資料處理監督作業

1.個資因應專案小組應針對個資的處理作業進行監督，包括依「資料安全維護檢核作業程序」之規定填寫「資料安全維護檢核表」進行對於資料安全措施的稽核作業及針對處理作業進行資料處理作業正確性的稽核，以確保所有處理均合於本規範及個資法之要求。

2.監督作業過程如發現公司處理不合於個資法蒐集、處理要件所取得之個人資料，或不合於特定目的之處理作業，應立即停止該資料之處理，並填寫「系統程式修改／新增申請單」提出對於該資料的刪除及後續矯正、預防作業。

3.監督過程如果發現嚴重違法的情事或相關處理作業之疏漏或系統漏洞及弱點，應立即回報管理階層。

四、**個人資料利用管理作業**

本公司於蒐集個人資料時應遵循以下作業程序

(一) 個人資料利用前管控作業

1. 新的利用方式或利用行為進行前應填寫資料利用之申請，個資因應專案小組應進行對該申請書之審查，並視其需求核准或經管理階層核准利用之行為。

(二) 個人資料利用監督作業

1.利用申請書核准後，資料利用人員，應依照申請書之核准範圍進營資料的利用，並將該資料利用之方式告知相關人員。

2.個資因應專案小組應依照申請書所核准之利用範圍進行對於個人資料利用的監督作業，當個人資料利用的行為超出該核准範圍時，應予以糾正，並提出矯正及預防計畫避免事件再次發生。

3.監督過程如果發現嚴重違法的情事或相關利用作業之疏漏或利用過程使用系統漏洞及弱點，應立即回報管理階層。

五、個人資利委外蒐集、處理、利用管理作業

(一) 委外作業管理

公司如需將個人資料進行委外的蒐集、處理、利用作業，應於委外事項進行前與該受委託單位(公司或個人)，進行委外作業的簽約，並依照【附件 4】委外處理個資合約範例進行合約的簽訂。

(二) 委外監督作業

1. 依照個人資料保護法施行細則第八條進行對於個人資料委外作業之監督作業。(詳【附件 9】委外作業安全管理檢核表)

2.個資因應專案小組應定期，要求受委託單位進行對於所受託之業務執行狀況進行相關的報告，並將此監督之結果做成紀錄備查。

3.個資因應專案小組應定期或於需要時針對受委託廠商進行稽核或現場稽核，以確保所有的個人資料委託處理之作業均符合公司之要求。

4.委外作業結束，個資因應專案小組應監督受委託廠商返還或銷燬公司已交付之個人資料，以確保個人資料之委外作業安全。

柒、控制重點

一、公司是否遵循個人資料保護法之規定，履行相關法定告知義務。

二、已蒐集之個人資料是否作適當且相關之處理，並依法或於合法之特定目的下進行妥善保存及刪除。

三、是否採取合理適當安全保護措施，以免個人資料遭遺失、盜用、毀損、竄改或揭露的風險。