

1、目的：

明訂公司資訊系統作業程序及責任、系統規劃、電腦病毒及惡意軟體之防範、軟體複製之控制、個人資料之保護、日常作業之安全管理、電腦媒體之安全管理、資料及軟體交換之安全管理等規範，週知全體同仁遵照，以確保公司資訊安全。

2、適用範圍：

全公司。

3、名詞定義：

無

4、相關文件：

電腦軟體管理作業辦法

資訊安全緊急應變實施辦法

電腦機房管理辦法

ERP 系統資料備份作業辦法

5、內容說明：

5.1 資訊系統作業程序及責任

5.1.1 資訊系統作業程序之訂定

5.1.1.1 本公司各資訊系統應由使用單位依需求，訂定系統作業程序，並以書面、電子或其他方式載明之，以確保公司同仁正確及安全地操作此資訊系統，並用以作為系統發展、維護及測試作業的依據。

5.1.1.2 系統作業程序應載明執行每一項作業的詳細規定，詳列如下：

5.1.1.2.1 如何正確地處理資料、檔案及處理的規則。

5.1.1.2.2 資訊系統作業時程的需求，包括與其他系統的相互關係、作業啟動的最早時間及作業結束的最晚時間。

5.1.1.2.3 處理電腦當機及發生作業錯誤之規定，以及其他資訊系統作業之限制事項。

5.1.1.2.4 如果遭遇非預期的問題時，與支援人員聯繫之步驟規定。

5.1.1.2.5 資料輸出處理的特別規定，例如：使用特別的文具，或是機密資料輸出之管理、電腦當機或作業錯誤時，輸出資訊之安全處理規定等。

5.1.1.2.6 電腦當機重新啟動及回復正常作業之程序。

5.1.1.2.7 資料重要性等級與資料保存期限，以作為資料備援政策、資料備份政策擬定的依據。

5.1.2 資訊安全事件之管理

5.1.2.1 應建立處理資訊安全事件之作業程序，並付予相關人員必要的責任，以便迅速有效處理資訊安全事件。

5.1.2.2 發生資訊安全事件之反應與處理作業程序：

5.1.2.2.1 電腦當機及中斷服務，應依資訊安全緊急應變實施辦法、ERP 系統資料備份作業辦法處理、ERP 系統異常處理作業辦法。

5.1.2.2.2 業務資料於平常作業時應確保完整與正確，若因不完整，或資料不正確導致的作業錯誤，應即修正。

5.1.2.2.3 機密性資料應依權限儲存及調閱，若遭侵犯，應即鎖定追蹤，對侵犯管道速提報再發防止方案，業務單位並對侵犯機密性資料人員提報懲處及依法追訴。

5.1.2.3 除正常的應變計畫外，資訊安全事件之處理程序，尚應納入下列事項

5.1.2.3.1 導致資訊安全事件原因之分析。

5.1.2.3.2 防止類似事件再發生之補救措施的規劃及執行。

5.1.2.3.3 電腦稽核軌跡及相關證據之蒐集。

5.1.2.3.4 與使用者及其他受影響的人員，或是負責系統回復的人員進行溝通及瞭解。

5.1.2.4 電腦稽核軌跡及相關的證據，應以適當的方法保護，以利下列管理作業：

5.1.2.4.1 作為研析問題之依據。

5.1.2.4.2 作為研析是否違反契約或是違反資訊安全規定的證據。

5.1.2.4.3 作為與軟體及硬體之供應商，協商如何補償之依據。

5.1.2.5 應以審慎及正式的行政程序，處理資訊安全及電腦當機事件。作業程序應該包括下列事項：

5.1.2.5.1 應在最短的時間內，確認已回復正常作業的系統及安全控制系統，是否完整及真確。

5.1.2.5.2 應向管理階層報告緊急處理情形，並對資訊安全事件詳加檢討評估，以找出原因及檢討改正。

5.1.2.5.3 應限定只有被授權的人員，才可使用已回復正常作業的系統及資料。

5.1.2.5.4 緊急處理的各項行動，應予詳細記載，以備日後查考。

5.1.3 資訊安全責任之分散

5.1.3.1 為降低因人為疏忽或故意，導致資料或系統遭不法或不當之使用，或遭未經授權的人員竄改，對關鍵性的資訊業務，應將資訊安全管理及執行的責任分散，分別配賦相關人員必要的安全責任。必要時，應建立相互制衡機制。

5.1.4 系統發展及系統實作之分開處理

5.1.4.1 系統發展及測試作業可能會有軟體變更及電腦資源共享之情形，為降低可能的風險，應將系統發展及系統實作的設施分開處理，以減少作業軟體或資料遭意外竄改，或是遭未經授權的存取。

5.1.4.2 系統發展及系統實作之分開處理，應考量下列安控措施：

5.1.4.2.1 系統發展及系統實作的軟體，應儘可能在不同的處理器上作業，或是在不同的目錄或領域下作業。

5.1.4.2.2 系統發展及測試作業應儘可能分開。

5.1.4.2.3 編輯器及其他公用程式不再使用時，不得與作業系統共同存放。

5.1.4.2.4 實作及測試用的系統，應使用不同的登入程序，以減少風險。

5.1.5 資訊作業委外服務之安全管理

5.1.5.1 資訊業務委外時，應於事前審慎評估可能的潛在安全風險（例如資料或使用者通行碼被破解、系統被破壞或資料損失等風險），並與廠商簽訂適當的資訊安全協定，以及課予相關的安全管理責任，並納入契約條款。

5.1.5.2 應納入資訊委外服務契約的資訊安全事項如下：

5.1.5.2.1 涉及機密性、敏感性或是關鍵性的應用系統項目。

5.1.5.2.2 應經核准始得執行的事項。

5.1.5.2.3 廠商如何配合執行機關業務永續運作計畫。

5.1.5.2.4 廠商應遵守的資訊安全規範及標準，以及評鑑廠商遵守資訊安全標準的衡量及評估作業程序。

5.1.5.2.5 廠商處理及通報資訊安全事件的責任及作業程序。

5.2 系統規劃

5.2.1 系統作業容量之規劃

5.2.1.1 電腦主機系統之效能、磁碟使用率、記憶體容量、檔案儲存、印表機及其他輸出設備及通信系統之使用狀況等，由資訊人員電腦主機管理人員隨時注意及觀察分析系統的作業容量，以避免容量不足而導致電腦當機。

5.2.1.2 對電腦作業容量需進行需求預測，預留預算及採購行政作業的前置時間，俾利進行前瞻性的規劃，及時獲得必要的作業容量。

5.2.2 新系統上線作業之安全評估

5.2.2.1 本公司任何新系統被認可及納入正式作業的標準，應執行下列事項：

5.2.2.1.1 應評估系統作業效能及電腦容量是否滿足公司的需求。

5.2.2.1.2 應檢查發生錯誤後之回復作業及系統重新啟動程序的準備作業，以及資訊安全事件之緊急應變作業完備與否。

5.2.2.1.3 應進行新系統正式納入例行作業程序之準備及測試。

5.2.2.1.4 應評估新系統的建置是否影響現有的系統作業，尤其是對系統尖峰作業時段之影響。

5.2.2.1.5 系統上線前，需檢查程式碼有無後門或木馬程式。

5.2.2.2 在發展重要的系統時，應確定系統的功能，以及確保系統的作業效能，使其足以滿足需求；例如，在系統發展的每一階段，應充分諮詢相關人員的意見。

5.2.2.3 新系統上線作業前，應執行適當的測試作業，以驗證系統功能符合既定的安全標準。

5.2.3 備份系統作業之規劃

5.2.3.1 對於本公司之每一應用系統，均應規劃資訊系統設備損害或電腦當機時，可維持公司業務繼續正常作業的替代性預備作業方法。

5.2.3.2 每一系統的備份系統作業需求，應在業務永續運作的基礎上，由系統的擁有者加以界定；資訊服務提供者亦應為每一項系統研訂適當的備份系統作業計畫。

5.2.3.3 應定期測試備份系統作業的設備及程序。

5.3 電腦病毒及惡意軟體之防範

為使本公司 ERP 電腦主機免於電腦病毒之侵襲，(1)禁止檔案資料匯入 (2)購買適合之防毒軟體或網路下載合法防毒軟體，安裝於個人電腦，必須定時自動更新相關病毒碼及掃毒引擎，可過濾含有病毒之文件及郵件，以減少病毒之威脅。

5.4 軟體使用及複製之管理

依「電腦軟體管理作業辦法」辦理。

5.5 個人資料之保護

本公司應依據電腦處理個人資料保護法等相關規定，審慎處理及保護個人資料。

5.6 日常作業之安全管理

5.6.1 資料備份

參考「ERP 系統資料備份作業辦法」。

5.6.2 系統作業紀錄

5.6.2.1 主機系統設定異動時需書面呈報經主管核准後執行，需填具「作業系統更新申請表」，保留相關異動記錄。

5.6.3 系統錯誤事項之處理及紀錄

5.6.3.1 本公司資訊人員，於接獲或發現電腦系統（含應用系統）錯誤發生後，應即檢視錯誤，判斷處理方式。

5.6.3.2 凡錯誤事件之處理，資訊人員無法處理需委外維修合約廠商處理需掌握處理時間性，並先知會使用單位讓使用者了解情況並採取應變措施。。

5.6.3.3 對於電腦作業錯誤事件，均應詳實記錄在「電腦異常作業記錄簿」，重大的錯誤事件，應上呈報告。

5.6.4 電腦作業環境之監測

本公司電腦機房作業環境之監測，另訂電腦機房管理辦法。

5.7 電腦媒體之安全管理

5.7.1 電腦媒體之安全管理

5.7.1.1 重要儲存媒體實體應做異地存放。

5.7.1.2 應儘量避免使用有明顯用途標示的資料儲存系統；電腦媒體儲存的資料內容，不應在媒體外部以明顯方式標示，以免被輕易地辨識。

5.7.1.3 可重複使用的資料儲存媒體，不再使用或不堪使用時，應將儲存的內容消除或銷毀。

5.7.1.4 儲存媒體應依製造廠商提供之保存建議環境及條件，存放在安全且符合保存標準的地方。

5.7.1.5 不再使用之重要媒體，應予銷毀並記錄處理方式。

5.7.2 機密性及敏感性資料之處理程序

5.7.2.1 本公司機密性及敏感性資料之處理，需依相關法規辦理。

- 5.7.2.2 本公司之機密性及敏感性資料，以電子方式處理或儲存時，應依存取權限進行處理。
- 5.7.2.3 以電子方式傳輸本公司機密性及敏感性資料時，需以加密、電子簽章、認證等安全方式處理。
- 5.7.2.4 本公司之機密性及敏感性資料，以電子方式儲存時，應存於安全性及穩定性較高之主機及週邊設備，並視需要對存放資料之主機設立實體保護或獨立門禁管制。
- 5.7.2.5 資訊累積一段時間再作彙總處理時，應特別注意及防止大量非機密性資料彙總成為敏感性或機密性資料。
- 5.7.2.6 機密性及敏感性資料之安全處理作業，應包括下列事項：
 - 5.7.2.6.1 輸出及輸入資料之處理程序及標示。
 - 5.7.2.6.2 依授權規定，建立收受機密性及敏感性資料的正式收文紀錄。
 - 5.7.2.6.3 確保輸入資料之真確性，及資料修改之不可否認性。
 - 5.7.2.6.4 儘可能要求收受者提出傳送之媒體已送達的收訖證明。
 - 5.7.2.6.5 分發對象應以最低必要的人員為限。
 - 5.7.2.6.6 為提醒使用者注意安全保密，應在資料上明確標示資料機密等級。
 - 5.7.2.6.7 應定期評估機密性及敏感性資料的發文清單，及檢討評估內容。
 - 5.7.2.6.8 應確保資訊系統內部資料與外部資料之一致性。
- 5.7.3 系統文件之安全
 - 5.7.3.1 系統流程、作業流程、資料結構及授權程序等系統文件，由系統負責人負責管理，以防止不當利用。
 - 5.7.3.2 系統文件的安全保護措施如下：
 - 5.7.3.2.1 應鎖在安全的儲櫃或其他安全場所。
 - 5.7.3.2.2 發送對象應以最低必要的人員為限，且應經文件管理者的授權。
 - 5.7.3.2.3 電腦產製的文件，應與其他應用檔案分開存放，且應建立適當的存取保護措施。

5.7.4 媒體處理之安全

5.7.4.1 儲存機密性及敏感性資料的電腦媒體，當不再繼續使用時，應予以銷毀（鎔毀、碎紙處理、將資料從媒體中完全清除等）。

5.7.4.2 機密性及感應性資料的處理過程，應以書面、電子或其他方式記錄之，以利事後查考及稽核。

5.7.4.3 需以安全方式處理的媒體項目，應包括以下項目：

5.7.4.3.1 輸入文件，例如電傳文件。

5.7.4.3.2 複寫紙。

5.7.4.3.3 輸出報告。

5.7.4.3.4 印表機色帶。

5.7.4.3.5 磁帶。

5.7.4.3.6 可攜帶的磁片、攜帶式隨身碟、磁帶、光碟等。

5.7.4.3.7 作業程序目錄。

5.7.4.3.8 測試資料。

5.7.4.3.9 系統文件。

5.7.4.3.10 其他。

5.7.4.4 委外處理的電腦文具、設備、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。

5.7.5 資料檔案之保護

5.7.5.1 資料檔案的重要性及保存期限由業務單位（依法）訂定。

5.7.5.2 重要的資料檔案，應適當設定其存取權限。

5.7.5.3 重要的資料檔案，應經常作完整之資料備份。

5.7.5.4 超過法定保存時限的檔案，可依相關規定刪除或銷毀，惟應事前考量對本公司造成之影響。

5.7.5.5 重要資料檔案，應建立資訊資源目錄，並應指定適當人員保管。

5.8 資料及軟體交換之安全管理

5.8.1 資料及軟體交換之安全協定

5.8.1.1 本公司與其它機關間進行資料或軟體交換，應訂定正式的協定，將機密性及敏感性資料的安全保護事項及有關人員的責任列入。

5.8.1.2 機關間資料及軟體交換的安全協定內容，應考量下列事項：

5.8.1.2.1 控制資料及軟體傳送、送達及收受的管理責任。

- 5.8.1.2.2 控制資料及軟體傳送、送達及收受的作業程序。
- 5.8.1.2.3 資料、軟體包裝及傳送的最基本的技術標準。
- 5.8.1.2.4 識別資料及確定軟體傳送者身分的標準。
- 5.8.1.2.5 資料遺失的責任及義務。
- 5.8.1.2.6 資料及軟體的所有權、資料保護的責任、軟體的智慧財產權規定等。
- 5.8.1.2.7 記錄及讀取資料及軟體的技術標準。
- 5.8.1.2.8 保護機密或敏感性資料的安全措施（例如使用加密技術）。
- 5.8.2 電腦媒體運送及傳輸之安全
 - 5.8.2.1 電腦媒體運送及傳輸過程，應有妥善的安全措施，以防止資料遭破壞、誤用或未經授權的取用。
 - 5.8.2.2 電腦媒體運送及傳輸，應考量的安全措施參考要項如下：
 - 5.8.2.2.1 應審慎選用安全及可信賴的運送或傳送機構或人員，報請權責主管人員同意，並於事前執行傳遞人員或機構的安全評估程序。
 - 5.8.2.2.2 運送的物品應有妥適的包裝，以防止傳送過程中受損。
 - 5.8.2.2.3 對於機密及敏感性的資料，應採取特別的安全保護措施。
 - 5.8.2.2.4 如委託本公司以外之人員或機構運送及傳輸電腦媒體，應事前訂定契約。
 - 5.8.2.2.5 電腦媒體運送及傳輸，應有簽送簽收記錄。
- 5.8.3 電子資料交換之安全
 - 5.8.3.1 本公司與其它機構間之電子資料交換之資料內容，需經資料擁有者（業務單位）之同意授權。
 - 5.8.3.2 本公司提供給其它機構之資料，不得超出實際需求之資料項目。
 - 5.8.3.3 本公司與其它機構間進行電子資料交換，應採行特別的安全保護措施，以防止未經授權的資料存取及竄改；資料電子交換如有安全及責任上的考量，應建立發文及收文證明的機制。

5.8.3.4 公司訂定的電子資料交換安全措施，應與電子資料交換的對象及資料加值服務業者共同協商，並徵詢電子資料交換相關組織之意見，以確保符合相關的標準。

5.8.4 電子辦公系統之安全

5.8.4.1 本公司採用之電子辦公系統，需具備流程控制、權限設定、使用者群組劃分等功能。

5.8.4.2 本公司各電子辦公系統之使用者，不得將帳號、通行碼等使用權利，借予他人使用。

5.8.4.3 電子辦公系統應考量的安全事項如下：

5.8.4.3.1 電子辦公系統如未能提供適當及足夠的安全保護措施，不應將敏感性資訊列入系統目錄。

5.8.4.3.2 對於特定個人（如主管或負責處理機密性或敏感性資訊的人員）的行程資訊等，不宜開放公開存取，並應予適當的限制。

5.8.4.3.3 應評估以電子辦公系統處理本公司重要業務的適當性（例如：評估以電子通信系統傳達命令及線上授權的妥適性。）

5.8.4.3.4 應建立被授權使用電子辦公系統的員工、其他機關的員工及訂有契約廠商人員的名單，並建立使用者存取系統權限等資訊。

5.8.4.3.5 特定的電子辦公設施，應限制只有特定人員才能使用。

6、附件：

6.1 主機系統異常處理單

6.2 作業系統更新申請單