

資通安全自評表

V1.0

公司名稱：	自評人員：	自評日期：
	查核人員：	查核日期：

**自評表填寫說明：**

- 廠商請於表頭填上自我評核之公司名稱，自評人員姓名，與自評日期。
- 廠商需勾選及填寫自我評核與佐證資料說明。
  - 自我評核部分，並非每個評核項目皆為「應符合」，廠商需按現況及風險評估結果勾選適當欄位。
  - 該項目若現況完全符合，請於【符合】欄位打勾「V」；若現況部分符合，請於【部分符合】欄位打勾「V」；若現況完全不符合，請於【不符合】欄位打勾「V」。
  - 若本要求中之「(✓) 原則上應符合」項目經風險評估後已由計畫主持人決定不適用，請於【不適用】欄位打勾「V」，未來於資安訪視期間須提供風險評估佐證資料。
  - 考量商業模式及製造業之特性，若有計畫因其服務特殊性而無法符合本要求中之「● 應符合」項目，請於【不適用】欄位打勾「V」並說明原因，未來於資安訪視期間須提出補償性措施並呈現相關證據，且須經計畫主持人簽核同意排除。
- 【佐證資料說明】欄位，請填寫該評核項目之具體控制措施內容並檢附證明資料，或說明不適用的理由。

自評項目	項目說明	自我評核				佐證資料說明	顧問查核結果			
		符合	部分符合	不符合	不適用		符合	部分符合	不符合	不適用
人員認知及訓練										
資安人員進用	資訊安全部門是否由貴組織主管指定至少 1 名人員擔任？	請受查驗計畫說明資安人員任用狀況								
會議招開	資訊安全部門是否至少每年召開 1 次資訊安全管理審查會議。	請受查驗計畫說明資安管理會議招開情形								
保密簽署	員工正式任用時，應簽定貴組織制定的聘僱契約，其中應陳述員工對資訊安全的責任，並依規定簽署保密合約。	受查驗計畫聘用時之保密簽署								
存取控制管理										
使用防火牆與 VPN	須有防火牆、入侵偵測等資安設備保護，若透過遠端連線進行管理則必須透過加密通道，登入時必須採用安全的身分鑑別機制。	請受查驗計畫提供網路架構圖，簡述防禦機制是否合理跟恰當。								
實體存取控制	應有實體安全的保護措施，外連線端口需最小化管理機制。	資通訊系統是否有該資產實體保護或操作保護機制。								
權限管理	針對核心系統的存取應控管並留存相關日誌紀錄。	保存核心系統存取紀錄								

防竄改機制	應確保資通訊系統內的資料(設定檔、程式碼、資料庫等)不被未經授權的篡改。	應有機制確保未經授權的人員篡改。									
保護資料之傳輸，使用及儲存	若存在機敏性資料時，無論傳輸、使用及儲存都應進行加密保護。	若資通訊系統中有機敏性資料，則在傳輸、使用及儲存都須採行適當之加密，並使用業界公認的加密方式。									
通訊與作業安全											
公用電腦限制	公用之個人電腦或終端機是否設定登入控管，以確保僅經授權人員可以使用，且應限定其存取資料之路徑、連線方式，及可使用之服務	公用之個人電腦是否應限定連線及存取									
強制使用強密碼	應建立密碼管理机制，系統應審核所使用之密碼強度，並提供密碼恢復及重置機制，管理机制包含： 1. 須更改初始密碼，並不允使用硬編碼之密碼或存在管理後門密碼。 2. 應要求密碼強度(至少包含長度、複雜度、密碼週期)，可參考NIST、OWASP及SANS之密碼規範。 3. 密碼失效鎖定機制(3次密碼輸入錯誤即鎖	各計畫依其特性評估是否排除適用。 如有使用密碼，密碼管控應至少須包含但不限於左述幾種。									

	定，至少 15 分鐘後解鎖)。 4.密碼需加密保存。 5.進行認證時，密碼不應以明碼方式直接顯示於畫面中。										
電腦更新	定期更新電腦作業系統及與軟體之重大更新檔	電腦定期更新									
保持軟體/ 韌體更新	資通訊系統應建立軟體、韌體安全性更新機制及部署時機，若更新部署失敗應可成功回復至前一個版本。	軟體更新應有安全機制以確保更新檔案的完整性。若更新失敗應可回復前一個正常版本。									
遠距系統使用	只有在已制定適當的安全控制措施，且控制措施符合安全政策時，始能批准遠距工作活動。	對於遠距工作場所之環境安全有相關之規範									
限制遠端對安全網路的存取	對於遠端連線應實施適當的存取管制，至少包含使用加密方式通訊、依工作性質給予低權限權、應保留遠端連線日誌。	若有遠端連線應有適當的管理機制，應包含不限於連線加密方式、使用者帳號權限小化、遠端連線應留存相關日誌。									
自我監測	資通訊系統應建立自我檢測功能，如完整性檢查、定期回報、系統異常偵測，若發生上述情況時應有發送通知機制。	系統自我監測功能									
監控及偵測容量使用情況	應監控全資通訊系統使用狀況，如：CPU、記憶體、儲存空間、	CPU、記憶體、儲存空間、頻寬使用率...等，若達到警戒值應									

	頻寬使用率...等，若達到警戒值應存日誌紀錄並進行通知。全資通訊系統需符合計畫自訂的可用性百分比。	存日誌紀錄並進行通知										
資料備份	應採取「321 原則」，重要檔案須保有三份備份，以兩種不同形式進行檔案存放，以及一份異地備份。	資料應採取321 備份原則										
加密備份	應識別重要的應用程式、設定檔、機敏資料並進行加密備份。	應識別出資通訊清冊中那些為重要應用程式(如程式碼、函式庫)、設定檔、機敏資料(如個資等)。識別出的重要檔案應進行備份並且加密保護。各計畫依其特性評估是否排除適用。										
日誌記錄保存												
日誌稽核管理	具備日誌與稽核機制，且須存查至少一年。	日誌存查稽核管理制度										
異常日誌紀錄	針對資通訊系統的異常狀況應有日誌紀錄。異常狀況可參考下列所示： 1.使用者登錄，註銷和失敗的身份驗證嘗試。 2.連接，中斷連線、連線嘗試失敗。 3.授權存取失敗。 4.存取機敏性資料。	計畫應就資通訊系統的異常狀況有所留存日誌以便日後查詢與分析。										

	5.從可移動媒體存取資料。 6.帳號權限的任何更改。 7.使用者新建、修改和刪除資料。 8.任何對系統變更的操作。 9.任何遠端操作。 10.安全更新失敗。										
紀錄存取機敏資料	針對機敏性資料的存取應控管並留存相關日誌紀錄。	各計畫依其特性評估是否排除適用。									
密鑰管理的職責分離	對於金鑰的產生、儲存與使用應保存日誌紀錄，宜採用職責分離方式管理金鑰。	對於金鑰的產生、儲存與使用應有留存日誌紀錄。其管理方式建議使用職責分離方式。									
資安系統開發與安全維護											
進行安全檢測	資通訊系統須於上線前及營運期間定期進行弱點掃描及滲透測試，高風險漏洞應被評估並依計畫可接受方式處理。	資通訊系統須於上線前進行弱點掃描及滲透測試，且訂定合適的資安檢測週期，並對發現之威脅與弱點採取對應之預防或應變措施。									
進行備援或備份之復原演練	應建立業務持續運作計畫(BCP)或災難復原計畫(DRP)，定期進行演練並持續改善。	對於資通訊系統應有 BCP 或 DRP 計畫(至少一個)。且須有定期演練紀錄，針對演練之過程缺失持續改善。									