資訊安全要求

為引導產業建立資訊安全認知與制度，要求申請企業建立資安防護機制，以保障我國軟體及資訊服務業者開發安全、可靠的前瞻技術或具市場應用價值之創新解決方案，帶動產業數位轉型。本計畫資訊安全要求如下。

壹、共同規範：

一、施作項目

（一）、 申請時應提出資安防禦機制與資訊安全規劃，包含定期審查服務流程並持續改善，以達到資安防護之目的。

1. 資訊安全規劃，包含網路管理、資料安全、存取控制、資安管理、營運持續、生命週期保護等等。
2. 資安產品功能包含防毒軟體、防火牆、弱點掃描、資料傳輸加密、AI 防毒監控、資安認驗證、資安情報、資安訓練、原始碼加密混淆器、伺服器安全監控等。

（二）、 計畫相關產品或服務如已有國家資安相關檢測標準，須採用通過資安驗證之產品。

（三）、 申請企業應由高階管理階層指派具決策主管人員負責協調資訊安全專案之計畫執行及資源配置。

二、注意事項

（一）、 補助計畫簽約時，資安防護工作倘由其他資安業者規劃執行，應提供與資安業者簽訂之「合約（契約書）」等佐證資料。

（二）、 資訊安全項目經費應占總經費合理比例，驗收時應提供支付資安企業之給付證明、說明於該案中所提供之產品及服務、解決哪些資安需求等。

（三）、 資安業者不應有過度再外包的情形（不得超過資安經費 50%）。

（四）、 使用的資安軟、韌、硬體產品，不得為中國大陸生產或開發。

（五）、 計畫內資安軟、韌、硬體產品，非國內（臺製）之資安產品佔比不得超過資安經費的 50%；若有特殊情形，須於計畫書、審查會中明文說明。

（六）、 資安經費編列倘包括公司內部資安人員，相關員工至少須具備以下一項(1)取得資安證照、(2)碩博士論文與資安相關、(3)曾在資安專業公司/機構從事資安相關工程、服務等滿一年、(4)其他可資舉證之相關資料。（註：資安專業不同於資訊專業。）

三、資安要求

申請企業須盤點與使用計畫相關產品或服務的企業間之資訊安全風險，包含網路管理、資料安全、存取控制、資安管理、營運持續、生命週期保護

等等面向，進行問題分析與提出最佳調整方案之建議，需含教育訓練、機制建立、系統導入、導入後查驗、資安架構圖，且建置及導入 35%以上應為國內業者產品及服務，計畫驗收至少須達必要要求之條件。並另敘明：

（一）、 資訊安全組織：請說明負責資訊安全計畫、執行、查核及改善之人員，並由管理階層負責協調專案資源。

（二）、 資訊安全計畫：請規劃資訊安全風險評估，可透過但不限於第三方單位執行原始碼檢測、黑箱檢測、滲透測試等，並針對重大威脅及脆弱性必須規劃資安防護解決方案。

貳、必要要求：

一、網路管理

（一）、 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。

二、資料安全

（一）、 啟用資料加密：對於資通訊系統中的資料應評估決定是否採取加密保護措施。

（二）、 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、使用和儲存都應進行加密保護。

（三）、 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。

（四）、 定期備份資料：應對資料進行備份。

三、存取控制

（一）、 實體存取限制：應有實體安全的保護措施，外連線端口需最小化管理機制。

（二）、 異常通報機制：若服務發生異常時（包含但不限於服務中斷、更新失敗），需有通知管道或機制。

（三）、 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。
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。

（四）、 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。

四、資安管理

（一）、 強制使用強密碼：應建立密碼管理機制，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，管理機制包含：

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。

（二）、 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。

（三）、 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。

（四）、 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。

五、營運持續

（一）、 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。

（二）、 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、零組件異常偵測，若發生上述情況時應有發送通知機制。

（三）、 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、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。

（四）、 進行多雲架構的服務備援機制：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。

六、生命週期保護

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。