應用系統資安控管表

紀錄編號： 填表日期： 年 月 日

|  |  |
| --- | --- |
|  系 統 名 稱 |   |

|  檢 查 項 目 | 資安控制項目 | 分析階段 | 設計開發 | 測試階段 | 維護階段 | 不適用或未採用說明 |
| --- | --- | --- | --- | --- | --- | --- |
| 符合或已採用者打勾(v)；不適用或未採用者(N/A)  |
| 依組織及業務需求，對資料和應用系統功能作存取權限控管；離職人員的系統帳號，自其離職生效日起即刻失效不可使用。 | 權限管理 |  |  |  |  |  |
| 規劃資料存放位置。原則上對所內提供服務的系統，Web Server與Database Server置於防火牆內；對所外服務的系統，Web Server置於DMZ區，Database Server置於防火牆內。 | 資料保護 |  |  |  |  |  |
| 重要之機密性資料(註1)應考量密碼控制措施或加密技術保護。 | 資料保護 |  |  |  |  |  |
| 資料若含極機密資訊，不得於行動裝置(註2)執行下載及滙出功能。 | 資料保護 |  |  |  |  |  |
| 連線本所主機之服務系統，應考量規劃透過本所SSO進行認證，登入後連續三小時未使用，則需重新認證。 | 安全系統工程 |  |  |  |  |  |
| 軟體委外開發，應與外包廠商確認程式碼所有權歸屬。 | 委外管理 |  |  |  |  |  |
| 軟體委外開發，應注意選擇聲譽良好的廠商。 | 委外管理 |  |  |  |  |  |
| 軟體委外開發，應要求外包廠商書面承諾對測試資料及相關文件善盡保密之義務。 | 委外管理 |  |  |  |  |  |
| 委外開發之軟體，外包廠商應符合本所規定之相關資安規範，並承諾程式原始碼不含特洛伊木馬程式(Trojan code)或其他危害資訊安全項目。 | 委外管理 |  |  |  |  |  |
| 資通安全法資通系統防護需求分級評估：(請依「資通系統防護需求分級原則」機密性、完整性、可用性及法律遵循性，四個構面防護需求分級，最後再將任一構面防護需求等級之最高者填入「評估結果」。) 四構面防護需求分級： 機密性：[ ] 高 [ ] 中 [ ] 普 完整性：[ ] 高 [ ] 中 [ ] 普 可用性：[ ] 高 [ ] 中 [ ] 普 法遵性：[ ] 高 [ ] 中 [ ] 普 評估結果： (請填：高/中/普) | 資通安全責任等級分級辦法-資通系統防護需求分級原則 |  |  |  |  |  |
| 依「防護需求分級評估」結果進行 「資通系統防護基準」。 | 資通系統防護基準 |  |  |  |  |  |
| 應遵守權責主管機關訂定的資料保密規範，及使用權責主管機關檢驗合格或認可的加密模組，以確保應用系統的安全功能。例如HTTPS或PKI機制。 | 資料加密 |  |  |  |  |  |
| 資料輸入、儲存及傳輸格式設計符合有效性及相依致性(如：數值是否超出上下限、是否為無效的文數字、格式、長度、代碼及檔案是否相依…等)。 | 資料驗證 |  |  |  |  |  |
| 具有極機密資料的系統增加存取資料的Log設計(應考慮有增、修、刪的異動紀錄)。 | 資料保護 |  |  |  |  |  |
| 利用系統提供的功能，做資料處理作業或批次控制，以達到檔案或資料更新處理後的一致性。 | 系統安全測試 |  |  |  |  |  |
| 當程式執行錯誤而產生異常狀況，系統應提供顯示警訊，防止進入下一步處理作業。 | 系統安全測試 |  |  |  |  |  |
| 轉檔過程中產生的暫存資料，應避免資料可未經授權修改，產生上下游資料不一致問題。 | 系統安全測試 |  |  |  |  |  |
| 驗證系統程式識別潛在的安全性瑕疵，進行安全性掃描，如：源碼檢測、滲透測試、弱點掃描。 | 系統安全測試 |  |  |  |  |  |
| 連結資料庫的系統密碼應妥善保存。 | 密碼保護 |  |  |  |  |  |
| 上線環境的系統存取控制措施，應適用在測試環境。 | 測試資料保護 |  |  |  |  |  |
| 保護及控制測試資料，避免包含機敏性及個資(不含公務個資)的真實資料進行測試；如需應用真實資料，真實資料被複製到測試環境時，應依複製作業的性質及內容，再取得書面授權後始能進行。 | 測試資料保護 |  |  |  |  |  |
| 自行或委外系統於開發、測試及上線階段，應有適當之區隔，並有個別的存取權限控制。 | 程式原始碼存取限制 |  |  |  |  |  |
| 應防止修改套裝軟體的行為，如確有必要修改套裝軟體時，應審查內控措施及完整性，以確保沒有被變更作業所破壞。 | 套裝軟體變更限制 |  |  |  |  |  |
| 套裝軟體需變更時，必須有完整測試及記錄。 | 套裝軟體變更限制 |  |  |  |  |  |
| 只有經過授權的人員，才能更新作業系統程式庫。 | 作業系統變更控制 |  |  |  |  |  |
| 應保留舊版的軟體，以作為緊急應變措施之用。 | 變更控制程序 |  |  |  |  |  |
| 檢視系統安全架構，確保應用系統變更作業不致影響或破壞，自行或委外系統原有的安全控制措施。 | 變更控制程序 |  |  |  |  |  |
| 應用系統變更作業時，應列出所需修正的電腦軟體、資料檔案、資料庫及硬體項目。 | 變更控制程序 |  |  |  |  |  |
| 系統文件在完成每次變更作業後，檢視及更新系統功能架構圖、作業流程圖，舊版的系統文件亦應妥善處理。 | 變更控制程序 |  |  |  |  |  |
| 建立軟體更新的版本控制機制。 | 變更控制程序 |  |  |  |  |  |
| 所有的系統變更作業請求，皆應建立紀錄。 | 變更控制程序 |  |  |  |  |  |
| 在適當的時機執行變更作業。 | 變更控制程序 |  |  |  |  |  |
| 作業系統變更時，審查應用程式控制措施和完整性程序，以確保沒有被作業系統變更作業所破壞。 | 變更控制程序 |  |  |  |  |  |
| 符合相關法令、規定及適用合約條款，確保資料保護與隱私。 | 資料保護 |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 系統負責人 |  | 直屬主管 |  | 日 期 |  |

註1：機密資料係指本所「保密辦法」明訂的列管項目。

註2：PC及筆電以外的手持行動裝置。

註3：符合或已採用者打勾(v)；不適用或未採用者填寫(N/A)，並於(不適用或未採用)欄位中說明。