附件1

**各機關對危害國家資通安全產品限制使用原則**

一、為推動資通安全管理法(以下簡稱本法)第五條第一項所定資通安全整體防護事宜，強化中央與地方機關（構）、公立學校、公營事業及行政法人(以下簡稱各機關)之資通安全防護，降低國家資通安全風險，特訂定本原則。

二、本原則所稱危害國家資通安全產品，指對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務。

三、本法主管機關應基於國家安全、國際情資分享、潛在風險及衝擊分析等因素，蒐集相關機關意見綜合評估，據以核定生產、研發、製造或提供前點產品之廠商清單。

本法主管機關應定期檢視前項核定之廠商清單，並依前項因素重新評估後，視需要調整。

四、各機關除因業務需求且無其他替代方案外，不得採購及使用第三點之廠商產品。

各機關必須採購或使用第三點之廠商產品時，應具體敘明理由，經本法主管機關核可後，以專案方式購置，並列冊管理及遵守下列規定：

 (一)應指定特定區域及特定人員使用。

 (二)不得與公務網路環境介接。

 (三)不得處理或儲存機關公務資訊。

 (四)測試或檢驗結果應產出報告。

 (五)購置理由消失，或使用年限屆滿應立即銷毀。

 五、各機關應依下列規定定期辦理資產盤點：

 (一)對本原則生效前已使用之第三點之廠商產品，應於廠商清單提供後三個月內列冊管理，不得與公務網路環境介接，並應移至非敏感或非重要環境。

 (二)前款之廠商產品已屆使用年限者，應於廠商清單提供後，即刻編列預算於該年度內汰除；未達使用年限者，應定明汰除期限。

 六、各機關應向所屬人員宣導使用危害國家資通安全產品之風險。

 七、中央目的事業主管機關應督導本法所定關鍵基礎設施提供者及政府捐助之財團法人，參考 本原則之規定辦理。

附件2

**南投縣交通工程及管理所停車場資訊安全管理規範**

112年7月14日

**壹、 目的**

為維護南投縣交通管理所(以下簡稱：本所)自營及委託經營停管場資料、系統、設備及網路安全，確保業務之正常運作，以避免民眾權益受損，訂定本規範。

**貳、 對象：本所委外及自營停車場**

**參、 本規範分為人員、實體環境、設備、資訊系統、電腦病毒、網路、軟體、個人資料、電腦媒體、全球資訊網、資安事件管理等11項，說明如下：**

一、人員安全管理及教育訓練

(一)對於可存取機密性與敏感性資訊或系統之人員離(調)職時，應適時取消或調整各項權限。

(二)定期參與本所資訊安全教育訓練，提升資訊安全管理能力。

二、環境及設備安全

(一)資訊及網路設備應安置於機櫃並上鎖。

(二)涉及停車場進出、收費及其他重要系統，應使用不斷電系統(UPS)。

(三)應注意電源及延長線之使用。

三、資訊系統作業安全管理

(一)應遵循本所資訊系統及網路架構規範配置相關設備。

(二)應使用Windows 10以上之作業系統。作業系統變更應評估其對應用系統之影響及安全問題。

(三)訂定資訊系統作業程序，包含不正常停機及發生錯誤或遭遇非預期性問題時之處理。

(四)作業系統及資訊系統應啟動稽核存錄功能，留存並妥善保管帳號登入、登出與特殊權限使用等電腦稽核紀錄（log）。

(五)定期執行必要之資料及軟體備份，備份資料應定期測試以確保其可用性。

(六)建立系統使用者帳號密碼及權限管理機制，原則上以一人一帳密為原則。

(八)密碼長度應至少八碼，並包含英文字母、數字與特殊符號之組合，並定期更換通行密碼，更新期限最長不得超過六個月。

(九)系統管理者帳號權限應至少每半年實施一次檢討及評估。

(十)使用軟體應遵守智慧財產權相關法令及契約約定。

(十一)停車場各系統若有需求需上全球資訊網，本所自營場應由本所統一控管，委外廠商應事先告知本所並確實做好資訊安全防護。

(十二)機密性、敏感性及個人隱私資料與文件不宜公布於全球資訊網。但因執行 業務致有公布之必要，且符合下列情形之一者，不在此限：

1、為防止他人權益之重大危害。

2、經當事人書面同意。

3、為增進公共利益。

(十三)提供民眾查詢之全球資訊網至少每年實施一次弱點檢核。

四、電腦病毒及駭客防範

(一)電腦應設定密碼保護、安裝防毒軟體，並即時更新系統與軟體漏洞修補。連接本處VPN之電腦，需安裝本所提供之防毒軟體，由本所定期更新。

(二)防毒軟體應更新病毒碼特徵，除線上即時防護外，每月至少實施一次完整 檔案掃瞄。

(三)電腦若疑似中毒或受駭，應立即拔除網路線，並通報管理單位處理。

(四)廠商進行維護時應採行必要的事前預防及保護措施，以預防及偵測電腦病毒、木馬及勒索病毒等惡意軟體之侵入。

(五)非必要不得使用可隨時攜帶及移動的電腦媒體(隨身碟或隨身硬碟)，若需使用需先進行申請及掃毒後方可使用。

五、網路安全管理

(一)開放外界連線作業之資訊系統及與外界連接網路之網路應設防火牆或其他必要安全設施。

(二)使用無線網路應與本處內部辦公作業網段區隔。

(三)禁止使用可攜式電腦或其他資訊設備連結防火牆之內之網路連接埠。

(四)需遠端登入本所伺服主機，應遵循本所規定申請核准。

(五)各系統間應實體隔離，若有資料交換需求，應設定帳號密碼及權限。

六、個人資料保護

(一)應依據「個人資料保護法」等相關規定，審慎處理及保護個人資訊。

(二)資訊系統應合理留存個人資料之新增、修改、刪除、資料匯出、列印等活動之操作紀錄。

七、資訊安全事件之管理

(一) 發生資訊安全事件應於發生1小時內通報本處。

(二) 應訂定備援方案並訂定復原程序、系統回復演練程序。

(三) 核心資訊系統應定期備份，包括完整系統備份及系統架構組態設定備份。

(四) 核心資訊系統復原程序應每年至少演練一次，以確認程序之有效性。

(五) 應配合本所每年2次之資安稽核(稽核項目表詳附件)。