資通安全政策

文件編號：TAD-ISMS-A-001
機密等級：一般

單　　位：交通部觀光署
版　　次：1.5

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	99.3.31		吳晴琳	初版發行
1.1	103.7.9	1,3,4,5,6	洪英瑋	修正第三條、第十一條、第十四條、第十五條、第十八條部分內容，並新增第十九條
1.2	105.9.26	3,4,6	吳晴琳	修正第三條、第七條及第十三條部分內容
1.3	108.9.19	4	吳晴琳	配合法令新增及廢止修正第七條部分內容
1.4	109.9.29	6,8	吳晴琳	增訂第十三條行動裝置之安全要求及第二十一條供應商管理
1.5	112.10.12		吳晴琳	因應觀光局組織改造為觀光署，調整相關名稱；將「資訊安全」用詞調整為「資通安全」(「資訊安全管理制度」用詞不調整)及修正部分文字

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

交通部觀光署資通安全政策

一、交通部觀光署及所屬(以下簡稱本署)為強化資通安全管理，建立安全及可信賴之各項資通應用系統，確保資料、系統、設備及網路安全及保障民眾權益，爰訂定本政策。

二、本政策係依據資通安全管理法及施行細則等有關法令，考量本署業務需求訂定，並以書面、電子或其他方式告知所屬員工及提供資通訊服務之廠商共同遵行。

三、為統籌資通安全管理等事項之協調及推動，成立資通安全暨個資保護委員會(以下簡稱本會)，下設資通安全執行小組、個人資料保護執行小組、內部稽核執行小組及緊急應變處理小組，本會之幕僚作業，由資訊業務單位負責。

四、資通安全定義

本署資產包含資訊資產、實體資產、軟體資產、服務資產、文件、人員、機關形象與榮譽等；安全則是利用主動或被動的各種方法，來保護或保存一個環境，使其活動的進行不受干擾。因此資通安全即為了避免因人為疏失、蓄意或自然災害等風險，運用一整套適當的控制措施，包括政策、實踐、步驟、組織結構和軟體功能等，來確保本署的資產受到妥善的保護。

五、資通安全目標

即確保資訊的機密性(只有經過授權的人才能存取資訊)、完整性(保證資訊及其處理方法的準確性和完整性)與可用性(確保經過授權的用戶在需要時可以存取資訊並使用相關資訊資產)，保護本署資訊資產免遭不當使用、洩漏、竄改、破壞等情事，確保資訊蒐集、處理、傳送、儲存及流通之安全。

六、資通安全範圍

本署所制定之資通安全政策及相關規定適用於本署所有作業及人員，包括正式員工、約聘僱人員、自然人、借調人員、工讀生、委外服務廠商(人員)、協力廠商(人員)、訪客及與本署連線作業之機關。

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

七、法令遵循

法令遵循為本署資通安全首要工作，下列法令為本署資通安全管理之重要依據，本署除依照相關法令之要求制定本政策外，並將法令之要求納入本署資通安全風險評估及風險管理之範疇：

(一) 個人資料保護法
(二) 國家機密保護法
(三) 檔案法
(四) 政府資訊公開法
(五) 資通安全管理法
(六) 電子簽章法
(七) 著作權法
(八) 商標
(九) 刑法

八、 依下列分工原則，賦予有關單位及人員權責：

(一) 資通安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。
(二) 資料及資通系統之安全需求研議、管理及保護等事項，由業務單位負責辦理。
(三) 資訊機密維護及安全稽核等事項，由政風單位會同相關單位負責辦理。

九、 本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：

(一) 人員管理及資通安全教育訓練。
(二) 電腦系統安全管理。
(三) 網路安全管理。
(四) 系統存取控制。
(五) 應用系統開發及維護安全管理。
(六) 資訊資產安全管理。
(七) 實體及環境安全管理。
(八) 業務永續運作計畫之規劃與管理。
(九) 資通安全稽核。

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

十、 人員管理及資通安全教育訓練

(一) 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

(二) 各業務主管人員，應負責督導所屬員工、委外人力、自然人、工讀生、委外廠商及人員等之資訊作業安全，並防範不法及不當行為。

(三) 針對管理、業務及資訊等不同工作類別之需求，定期辦理資通安全教育訓練及宣導，建立員工資通安全認知，提升資通安全水準。

(四) 負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

十一、電腦系統安全管理

(一) 辦理資通訊業務委外作業，應考量其業務活動或專案性質於事前研提適當之資通安全需求，明訂廠商之資通安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。

(二) 對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

(三) 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。

(四) 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

(五) 定期針對核心系統進行弱點掃描並謹慎完成重大弱點修補作業。

(六) 採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資通安全規範，研提資通安全需求，並列入採購規格。

十二、網路安全管理

(一) 開放外界連線作業之資通系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

(二) 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

(三) 訂定電子郵件使用規定，機密性資料及文件未加密不得以電子郵件或其他電子方式傳送。

十三、行動裝置安全

(一) 公務資料，有以行動裝置(含筆記型電腦、智慧型手機、平板電腦等)處理或儲存者，應設定安全防護機制，包括(但不限於)加密、上鎖、定期更新軟體版本(含弱點修補)、安裝防毒軟體等。

(二) 需以行動裝置作業者應取得核准，並遵循本署資通安全規範辦理。

十四、系統存取控制

(一) 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者相關權限及責任。

(二) 離(休)職人員，應取消各項資訊資源之所有權限，並列入離(休)職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

(三) 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼應訂定複雜度密碼並定期更新。

(四) 系統服務廠商以遠端登入方式進行系統維修者，應向本署申請並經許可，始可登入。

十五、應用系統開發及維護安全管理

(一) 自行或委外開發系統，應在系統生命週期之初始階段，即將資通安全需求納入考量；系統之維護、更新、上線執行、版本異動作業及專案管理等，應予安全管制，並經安全檢測及驗證，避免不當軟體、後門、電腦病毒或敏感資料外洩等危害安全之風險產生。

(二) 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

(三) 委託廠商建置及維護重要之軟硬體設施，應在本署相關人員監督及陪同下始得為之。

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

十六、資訊資產安全管理

(一) 建立與資通系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。

(二) 依據國家機密保護、個人資料保護及政府資訊公開等相關法規，建立資通安全等級之分類標準，以及相對應的保護措施。

(三) 已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

(四) 建立資訊資產相關之風險評估方法，以識別可能產生之內、外部風險，並進行風險管理。

十七、實體及環境安全管理

就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

十八、業務永續運作計畫之規劃與管理

(一) 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

(二) 建立資通安全事件緊急處理機制，在發生資通安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

(三) 針對本署機房所管系統，訂定備份計劃，並定期執行災難回復演練計劃，並在結束後改善回復缺失。

(四) 依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資通安全措施。

十九、資通安全稽核

(一) 應就本署業務性質確立稽核項目及範圍，並訂定相關之稽核計畫或作業程序。

(二) 為使資通安全政策能落實，應定期或不定期進行資通安全內部及外部稽核作業，並實施有效性量測，以確保達成資通安全目標。

二十、本署資通安全管理制度之決議事項，必要時可提報主管機關。資通安全暨個資保護委員會、主管機關(或法令、法規要求)、目的事業管轄業者、委

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

外廠商或專家學者等與執行資通安全管理制度相關之利害關係人如有資通安全相關回饋事項，可列入資通安全暨個資保護委員會議討論。

二十一、供應商管理

(一) 資通訊業務相關供應廠商(包括系統開發與維護、軟硬體設備建置與維護等)之服務條款，應經審核始得進行委外作業。

(二) 不得將應用系統正式資料未經適當處理而置於委外廠商所屬之作業環境中進行測試，其因特殊情況需要者，應有適當之安全防護措施。

(三) 本署委外管理應依據「資通安全管理辦法施行細則」第四條款，委外辦理資通系統之建置、維運或資通服務之應注意事項辦理。

二十二、本政策應至少每年評估 1 次，以反映政府法令、技術及業務等最新發展現況，確保資通安全實務作業之有效性。

二十三、本政策自奉核定後實施，修訂時亦同。

本文件為交通部觀光署專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。