交通部觀光署花東縱谷國家風景區管理處

資訊安全暨個人資料保護管理政策

文件編號：ELV-ISMS-A-001
機密等級：一般
版　　次：1.2
發行日期：中華民國 112 年 10 月 19 日

文件制／修訂記錄

版次	制/修訂 日期	制/修訂內容 摘要說明	修訂 頁次	修訂者	備註
1.0	106.11.29	初版發行		推動委員會	
1.1	109.10.22	增修本政策目標內容	p.1、2	推動委員會	
1.2	112.10.19	因應上級組織改革調整文字觀光局改為觀光署	All	推動委員會	

【目　　錄】

一、目的

為確保交通部觀光署花東縱谷國家風景區管理處（以下簡稱「本處」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅；並落實個人資料之保護及管理並符合「個人資料保護法」之要求，特訂定本政策。

二、適用範圍

1. 本政策適用範圍為本處之全體同仁、委外服務廠商（含合作廠商、承包商）、資料使用者(含保管者)與訪客等均適用之。
2. 資訊安全管理範疇應建置符合ISO 27001 國際標準之資訊安全管理系統（ISMS），考量組織環境、領導、規劃、支援、運作、績效評估、改善，並應涵蓋 14 項領域，以避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本處造成各種可能之風險及危害，各領域分述如下：
   (1) 資訊安全政策
   (2) 資訊安全組織。
   (3) 人力資源安全。
   (4) 資產管理。
   (5) 存取控制。
   (6) 密碼學。
   (7) 實體與環境安全。
   (8) 運作安全。
   (9) 通訊安全。
   (10) 系統獲取、開發及維護。
   (11) 供應者關係
   (12) 資訊安全事件管理。
   (13) 營運持續管理的資訊安全層面。
   (14) 遵循性。

三、目標

1. 為維護本處資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全，期藉由本政策保護本處業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
2. 保護本處業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
3. 建立本處業務永續運作計畫，以確保本處資訊業務服務之持續運作。
4. 建立本處資訊安全事件管理程序，以降低因事件所造成之損害，從而建立事件學習機制，藉以避免類似資訊安全事件重複發生。
5. 依「資通安全管理法」、「資通安全管理法施行細則」、「花東縱谷國家風景區管理處資訊安全政策」、「花東縱谷國家風景區管理處資通安全處理制度」訂定資通安全維護計畫。
6. 資通安全經費、資源之配置情形每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。
7. 依行政院核定資通安全責任等級分級辦法，本處屬 C 級機關，每兩年至少辦理 1 次資通安全健診。
8. 確保本處各項業務服務之執行須符合相關法令或法規之要求。
9. 依「個人資料保護法」、「個人資料保護法施行細則」要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。
10. 為保護本處業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
11. 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

四、責任

1. 本處應成立資訊安全組織統籌資訊安全事項推動。

2. 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。
3. 本處全體同仁、委外服務廠商、資料使用者(含保管者)與訪客等皆應遵守本政策。
4. 本處全體同仁、委外服務廠商及資料使用者(含保管者)均有責任透過適當通報機制，通報資訊安全事件或弱點。
5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本處之相關規定進行議處。

五、個人資料之保護

1. 本處應成立個人資料保護組織，明確定義相關人員之責任與義務。
2. 本處應建立與實施個人資料管理相關文件，以確認本政策之實行；全體員工及委外廠商應遵循個人資料管理之規範與要求。
3. 本處係以嚴密之措施、政策保護當事人之個人資料，包括但不限於本處之所有員工,均受有完整之個資法、或隱私權保護之教育訓練，本處之委外廠商或合作廠商與本公司業務合作時，均簽有保密契約，使其充分知悉個人資料保護之重要性及洩露個資相關之法律責任，倘有違反保密義務之情事者，將受嚴格之內部懲處或嚴重之違約求償，並追究其民、刑事法律責任。
4. 本處因營運所需取得或蒐集之包括但不限於個人之姓名、出生年月日、國民身分證統一編號（護照號碼）、特徵、指紋、婚姻、家庭、教育、職業等個人資料，應遵循我國個人資料保護法（以下簡稱個資法）等法令，適當、公平與合法地從事個人資料之蒐集與處理。且依個資法第 5 條規定，對於個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

5. 本處所蒐集、處理之個人資料，應遵循我國個資法及本處個資管理制度之規範，且個人資料之使用為本處執行業務所需，方可為本處承辦同仁利用。
6. 本處取得之個人資料，如有進行國際傳輸之必要者，定謹遵個資法第 21 條及相關規定且不違反國家重大利益、不以迂迴方法向第三國傳輸或利用個人資料規避個資法之規定等原則辦理。又，倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本處將不進行國際傳輸，以維護個人資料之安全。
7. 當本處接獲個人資料調閱或異動之需求時，應依個資法及本處所訂之程序，於合法範圍內進行當事人之個人資料。

六、利害相關團體之需求與期望

本處資訊安全管理制度之決議事項，應納入「資通安全暨個資保護推動委員會」管理審查會議報告，且會議紀錄於必要時將提報主管機關。推動委員會、主管機關(或法令、法規要求)、或專家學者等利害關係人如有資訊安全相關回饋事項，應將列入管理審查會議之討論議題。

七、審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展情況，確保本處業務永續運作之能力。資安組織、主管機關(或法令、法規要求)、或專家學者等利害關係人如有資訊安全相關回饋事項，應將列入管理審查會議之討論議題。

八、實施

本政策由「資通安全暨個資保護推動委員會」擬案並經處長核准後實施，修訂時亦同。