資訊安全暨個人資料保護管理政策

文件編號：ML-ISMS-A-01
機密等級：一般

單　　位：茂林國家風景區管理處
版　　次：1.4
發行日期：112 年 09 月 15 日

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	107.09.01		資料通訊暨個人資料安全處理小組	初版發行
1.1	108.09.01	1	資料通訊暨個人資料安全處理小組	修訂 3.5
1.2	109.09.22	2	資料通訊暨個人資料安全處理小組	修訂 5.1.2 增訂 5.1.7
1.3	112.06.20	3	資料通訊暨個人資料安全處理小組	刪除原管理指標 5.2.3、5.2.4、5.2.4、5.2.6、5.2.7，增訂 5.1.7、5.2.3、5.2.4、5.2.4、5.2.6、5.2.7
1.4	112.09.15	1~4	資料通訊暨個人資料安全處理小組	修訂組織名稱

目　錄

1 目的

為確保交通部觀光署茂林國家風景區管理處（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，以作為實施各項資訊安全措施之標準。透過本資訊安全政策之制定，明確宣示高階主管支持資訊安全之決心，並使相關人員有所依循。本政策整合本處原「茂林資訊安全政策及管理準則」之目標，餘詳參本處「管理系統文件列表」相關文件。

2 適用範圍

2.1 本政策適用範圍為本處之全體同仁、委外服務廠商、資料使用者(含保管者)與訪客等。

2.2 資訊安全管理範疇涵蓋 14 項領域，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。

3 目標

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，期藉由本政策之實施以達成下列目標：

3.1 建立安全及可信賴之資訊化作業環境，確保本處電腦資料、系統、設備及網路之安全，以保障本處業務永續運作。

3.2 保護本處業務服務之安全，確保資訊需經授權人員合法存取資訊，維護機密性。

3.3 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。

3.4 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。

3.5 確保本處各項業務服務之執行須符合資通安全管理法等相關法令或法規之要求。

3.6 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。

3.7 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。

3.8 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。

3.9 定期針對個人資料流程進行風險評鑑，鑑別可承受風險等級。

3.10 落實遵守資訊安全有關法律及規定，避免使用非法軟體。

3.11 提供員工資訊安全訓練，強化整體安全認知。

3.12 建置資訊安全控管設備及時偵測安全漏洞以防止電腦駭客入侵及病毒破壞。

4 責任

4.1 本處應成立資訊安全組織統籌資訊安全事項推動。

4.2 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。

4.3 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。

4.4 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。

4.5 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。

5 管理指標

為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

5.1 定量化指標

5.1.1 確保本處資訊服務可用性之要求如下：

5.1.1.1 資訊機房維運服務達全年服務時間 97%以上。

5.1.1.2 關鍵業務系統服務達全年服務時間 95%以上。

5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每年不得超過次數如下：

5.1.2.1 資訊機房維運服務中斷，每季不得超過 3 次。

5.1.2.2 關鍵業務系統服務中斷，每季不得超過 3 次。

5.1.3 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過工作小時要求如下：

5.1.3.1 資訊機房維運服務中斷，每次最長不得超過 6 工作小時。

5.1.3.2 關鍵業務系統服務中斷，每次最長不得超過 8 工作小時。

5.1.4 應適當保護本處資訊資產之機密性與完整性，每年至少需進行乙次風險評鑑及風險管理。

5.1.5 為確保本處資訊安全措施或規範符合現行法令、法規之要求，每年至少需稽核乙次。

5.1.6　演練業務永續運作計畫每年至少需進行乙次，以確保本處資訊業務服務得以持續運作。

5.1.7　為確保本處資訊安全措施或規範符合現行法令、法規之要求，每二年辦理 1 次資通安全健診作業。

5.1.8　為確保資訊機房設施之環境安全，非授權進入機房之人員進出登記，每年未落實次數不可超過 3 次。

5.2　定性化指標

5.2.1　應定期審查本處資訊安全組織人員執掌，以確保資訊安全工作之推展。

5.2.2　應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。

5.2.3　為確保資訊資產已受適當之保護，重要資訊系統每年執行帳號審查作業。

5.2.4　為確保資訊系統開發之安全需求，每年執行弱點掃瞄作業。

5.2.5　為確保管理制度落實之有效性，每年確實執行防毒與日誌管理相關作業之有效性。

5.2.6　為確保管理制度落實之有效性，每年確實執行內外部稽核之改善結果。

5.2.7　為確保管理制度落實之有效性，每年確實執行供應商(委外)稽核作業。

6　個人資料之保護

6.1.1　本處已成立個人資料保護組織，明確定義相關人員之責任與義務。

6.1.2　本處已建立與實施個人資料管理制度（Personal Information Management System，以下簡稱 PIMS），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制度（PIMS）之規範與要求。

6.1.3　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，應接受個資保護、或隱私權保護或資安相關之教育訓練，本處之委外廠商或合作廠商與本處業務合作時，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。

6.1.4　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。

6.1.5　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營運或業務所需，方可為本處承辦同仁利用。

6.1.6　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。

6.1.7　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。

7　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。

8　實施

本政策經「資料通訊暨個人資料安全處理小組」核定後實施，修訂時亦同。