



桃園市大溪區公所

安全管理政策

文件編號：	ISMS-L1-001
版次：	1.1
實施日期：	115年3月23日
機密等級：	公開

簽核欄	
審查	
核定	

文件制/修訂履歷

制/修訂版次	制/修訂日期	制/修訂說明	修訂單位	修訂人	備註
1.0	113/09/30	初版發行	秘書室	林玉芳	
1.1	115/03/23	因應修法改版	秘書室	林玉芳	參考文件異動

目 錄

壹、	目的.....	1
貳、	適用範圍.....	1
參、	權責.....	1
肆、	定義.....	1
伍、	作業程序.....	2
陸、	公布實施.....	3
柒、	參考文件.....	4
捌、	使用表單.....	4

壹、目的

桃園市大溪區公所（以下簡稱本公所）為確保資通資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資通資產遭竊、不當使用、洩漏、竄改或毀損等風險，並建立資訊安全管理系統，特訂定資通安全政策（以下簡稱本政策），本政策未規定事項依政府其他資通安全法規辦理，以達成資通資產之機密性、完整性與可用性。

貳、適用範圍

- 一、本公所同仁、委外服務廠商及第三方使用者。
- 二、本公所資訊相關資產。

參、權責

- 一、本公所資通安全長：核定本政策。
- 二、資通安全推動組織職責如下：
 - （一）安全管理政策內容研討、文件編修及公布事宜。
 - （二）安全管理政策得以召開管理審查會議或採書面審查方式進行。

肆、定義

- 一、安全管理政策：符合組織目的，提供欲達成資通安全目標，並滿足持續改善資通安全之承諾事項。
- 二、資通安全：應用管理程序及安全防護技術於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由列表機所列印之各式報表，俾能在資訊蒐集、處理、傳送、儲存及流通之過程中，確保資產之機密性、完整性與可用性。
- 三、個人資料：指自然人之姓名、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、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得

以直接或間接方式識別該個人之資料。

四、機密性 (Confidentiality)：指使資訊不可用，或不揭露予未經授權之個人、個體或過程的性質，確保只有經過授權的人才能存取資訊資產。

五、完整性 (Integrity)：指保護資產的準確度 (Accuracy) 及完全性 (Completeness) 的性質，確保資訊資產之處理方法的準確性及完整。

六、可用性 (Availability)：指經授權個體因應需求之可存取及可使用之性質，確保經授權之使用者在需要時，可以使用資訊資產。

伍、作業程序

一、依「資通安全責任等級分級辦法」規定，本公所資安責任等級為 C 級機關，將訂定相關程序並落實執行應辦事項，以符合 C 級機關相關法規遵循之要求。

二、本公所欲達成之資通安全目標如下：

(一) 量化型目標：

1. 資通系統可用性達 95% 以上。(中斷時數/總運作時數 \leq 5%)
2. 重大資安事件(第三、四級資安事件)不得發生超過 3 件。
3. 社交工程演練合格率達 95% (點閱人員/測試人員 \leq 5%)

(二) 質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

三、本公所為達成前開資通安全目標，預計採取以下安全管理政策：

- (一) 成立資通安全推動組織，負責資通安全保護制度之建立及推動事宜。每年應至少召開 1 次會議，必要時得召開臨時會，以確保資通安全之安全維護整體持續改善。
- (二) 訂定有效性之測量項目及方法，以達到本公所資通安全目標。
- (三) 識別各項資產作業流程的潛在風險，採取必要之控制要項進行改善，進而達到降低、迴避、轉移風險，以防範相關資安事件之發生。
- (四) 應鑑別出內部與外部的關注方，以及該關注方參與組織資料之安全保護程度，並明訂工作人員的職責及權責。
- (五) 應識別供應商所提供之產品與服務類型，須符合存取資訊或資訊處理設施之各項資通安全要求，並明訂於合約與協議中及定期審查。
- (六) 應建立設備、資料安全及人員管理規範及資安事故之通報與應變機制。
- (七) 應建立資料安全稽核及必要之使用紀錄、軌跡資料及證據之保存機制，以盡善良管理人之責任。
- (八) 確保同仁接受資通安全認知教育訓練，提升整體資安能量。
- (九) 訂定內部稽核計畫，檢視本公所資通安全管理措施執行情形，並依稽核報告採取適當矯正措施。

陸、公布實施

本政策應依業務變動、技術發展及風險評鑑之結果，每年至少評估一次作成審查紀錄，並持續改進其有效性及適切性，以符法令法規、技術及本公所營運要求。本政策評估審查結果應經「資通安全推動組織」審議通過，資通安全長核定後實施。

柒、參考文件

- 一、國家資通安全發展方案
- 二、資通安全管理法
- 三、資通安全管理法施行細則
- 四、資通安全責任等級分級辦法
- 五、資通安全事件通報應變及演練辦法
- 六、資通安全情資分享辦法
- 七、公務機關所屬人員辦理資通安全事項作業辦法
- 八、ISO/IEC/ CNS 27001 資通安全管理制度資通安全、網宇安全及隱私保護
—資通安全管理系統—要求事項

捌、使用表單

無