

桃園市政府經濟發展局

安全管理政策

文件編號：	ISMS-L1-001
版次：	V1.0
實施日期：	113年9月20日
機密等級：	公開

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	5

壹、目的

桃園市政府經濟發展局(以下簡稱本局)為強化資通安全管理，建立安全及可信賴之資訊環境，確保資料、系統、設備及網路安全之機密性、完整性及可用性，並確保機關業務職掌及資訊服務均能合理的蒐集、處理，以達「資安政策目標」特訂定本安全管理政策(以下簡稱本政策)，以為遵循。

貳、適用範圍

- 一、本局同仁、委外服務廠商及第三方使用者。
- 二、本局資訊相關資產。

參、權責

- 一、資通安全管理推動小組職責如下：
 - (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。
- 二、本局資通安全長：核定本政策。

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，本局資安責任等級為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、本局資通安全政策：

(一)本局依據可能影響資訊安全的內外部議題，與關注方對於資訊安全之要求事項，擬定完整的資訊安全管理制度。

(二)本局各項資訊安全管理規定必須遵守政府相關法規(例如：刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等)之規定。

(三)由「資通安全管理推動小組」負責資訊安全制度之建立及推動事宜。

(四)定期實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

(五)新資訊系統應於建置前將資訊安全因素納入，防範危害系統安全之情況發生。

(六)建立辦公區域實體及環境安全防護措施，並定期施以相關維護。

(七)明確規範資訊系統之使用權限，防止未經授權之存取行為。

(八)訂定資通安全之內部稽核計畫，定期檢視個人電腦使用情形及資訊安全制度落實情形。

(九)訂定資通安全之營運持續計畫並實際演練，確保本局業務持續運作。

(十)本局所有人員負有維持資訊安全之責任，且應遵守相關之資訊安全管理規定。

三、為符合本局資通安全政策及完善各項資安防護與達成永續發展目標，採取適當管理作為及執行規劃：

(一)成立資通安全管理推動小組，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，以達到本局資通安全目標。

(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)定期對同仁實施資通安全認知宣導，並針對資安專責(職)人員及資訊人員，辦理適當之教育訓練。

(九)訂定內部稽核計畫，檢視本局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、技術及本局營運

要求。本政策經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、資通安全事件通報及應變辦法。
- 六、資通安全情資分享辦法。
- 七、資通系統籌獲各階段資安強化措施。
- 八、政府機關雲端服務應用資安參考指引。
- 九、國家機密保護法。
- 十、國家機密保護法施行細則。
- 十一、個人資料保護法。
- 十二、個人資料保護法施行細則。
- 十三、公務人員任用法。
- 十四、公務人員服務法。
- 十五、各機關職務代理應行注意事項。
- 十六、公務機關所屬人員資通安全事項獎懲辦法。
- 十七、文書處理手冊。
- 十八、政府採購法。
- 十九、機關檔案管理作業手冊。
- 二十、桃園市市有財產管理自治條例。
- 二十一、桃園市市有財產產籍管理作業手冊。
- 二十二、桃園市政府資通系統開發及維運安全作業原則。
- 二十三、桃園市政府及所屬各機關學校人員資通安全事項獎懲基準。

二十四、國際標準 ISO/IEC/CNS 27001(Information technology-Security techniques-Information security management systems-Requirements)。

二十五、國際標準 ISO/IEC 27005 資訊安全風險管理。

二十六、國際標準 ISO 31000 風險管理。

捌、使用表單

無