# 金城鎮公所訊安全政策要點

101.9.18 修訂

金城鎮公所（以下簡稱本機關）為強化資訊安全管理，確保資料、系統、設備及網路安全，於有形無形（軟、硬體、文件、資料和流程）之可用資訊資產完整性、可靠性、機密性，提供相對之安全及可用性措施，特訂定本要點。

一、本要點適用本所各課室及使用本所網路設備之單位

二、本政策係依據行政院及所屬各機關資訊安全管理要點等有關法令，考量本機關業務需求，參考行政院及所屬各機關資訊安全管理規範、金門縣政府 96 年 10 月 11 日 1 府研資字第 0961200413 號函、97 年 5 月 12 日府研資字第 0970026985 號函訂定，並以書面、電子或其他方式通知員工及與本機關連線作業之有關機關（構）、廠商有所規範及遵循。

三、為統籌資訊安全管理等事項之協調、推動及監督，幕僚作業由行政課負責。

四、本政策之實施範圍如下：

1. 資訊資產之安全及風險管理。

2. 人員安全管理及資訊安全教育訓練。

(1). 對資訊相關職務及工作，應進行安全評估，於工作任務指派時，審慎評估其適任性，簽署保密協定，以確保系統之安全、順利運作。

(2). 針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知及法律責任與遵循，正確使用資訊處理設備，以提升資訊安全水準。

3. 實體及環境安全管理。

4. 個人電腦安全管理。

5. 主機系統安全管理。

(1). 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定要求廠商遵守。

(2). 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。

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

6. 網路安全管理。

(1). 開放外界連線作業之資訊系統，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。

(2). 與外界網路連接之網點，應以防火牆及其他必要安全設施作實體隔離，控管外界

與內部網路之資料傳輸與資源存取。

(3).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。

(4).訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

7.存取控制安全管理。

(1).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之相關權限及責任。

(2).離（休）職人員，應立即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。

(3).建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過三個月為原則。

(4).對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，賦予相關安全保密責任。

8.系統發展及維護安全管理。

9.資訊安全事故管理。

10.業務永續運作計畫之規劃及管理。

11.資訊安全稽核及遵循性管理。

(1).建立與資訊系統有關之資訊資產目錄，訂定資訊資產之項目、擁有者及安全等級分類等，且由專人負責並規範其權責。

(2).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，建立資訊安全等級之分類標準，以及相對應之保護措施。

(3).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。

五、本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

六、本要點自發布日起施行，修訂時亦同。