基隆市安樂地政事務所
資訊安全政策

中華民國 99 年 12 月 1 日訂定

壹、 依據

本政策係依據「行政院及所屬機關資訊安全管理要點」、「行政院所屬各機關資訊安全管理規範」、及「基隆市政府地政處資訊安全政策」，並考量本所業務需求制定，以確保地政資料、系統、設備及網路安全。

貳、 資訊安全定義

保存資訊的機密性、完整性及可用性亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質;維護資訊軟硬體設備與網路系統之安全及加強作業人員資訊安全之認知，避免資訊資源不當使用、洩漏、竄改、破壞等情事，防範各種來自內部或外部之威脅，以達到資訊安全之目的。

參、 資訊安全目標

一、確保地政資料之機密性及防止非法使用
二、確保地政資訊系統之完整性、可用性及安全性
三、確保地政資訊業務運作之有效性及持續性

肆、 資訊安全範圍

一、資訊資產安全管理
二、人員管理及資訊安全教育訓練
三、系統存取控制
四、資訊安全權責分工
五、環境安全管理
六、電腦系統安全管理
七、系統發展及維護安全管理
八、網路安全管理
九、資訊安全稽核

伍、 資訊安全組織

成立「地政資訊安全處理小組」，統籌資訊安全政策、計畫，資源調度，系統資料之安全需求、使用管理及保護等事項之協調、研議。

陸、 資訊安全管理作業規定

一、資訊安全教育訓練

應定期或不定期辦理資訊安全教育訓練及宣導，以提高員工資訊安全意識，促其遵守資訊安全規定。

二、系統存取控制

1、 建立系統使用者註冊管理制度，加強通行密碼之管理，其密碼更新周期以不超過三個月為原則。
2、 人員職務異動或調整應依系統存取授權規定，限期調整其權限；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。
3、 電腦設備應設置螢幕保護機制，及設定密碼保護，並於離開操作後限定時

間內啟動。

4、 未經授權禁止於電腦機房內使用行動式電腦設備，及以遠端連線方式存取資料。

三、電腦病毒防範之規定

機關內部之資訊設備應安裝防毒軟體，並定期進行掃毒及病毒碼更新等工作。

四、系統維護安全管理

1、 對廠商之系統建置及維護人員,應規範及限制其可接觸之系統與資料範圍,如基於實際作業需要，得核發臨時性之系統通行密碼供廠商使用，作業完畢後立即取消其使用期限。

2、 委託廠商建置及維護重要軟硬體設備，應在本所相關人員監督及陪同下始得為之。

五、網路安全管理

1、 採實體隔離方式區隔內、外部網路，以提高地政網路之安全性。

2、 設立防火牆控管外部與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。

3、 更新網路及資訊設備防毒病毒碼，及執行安全弱點修補工作，以提高資料之安全性及正確性。

4、 機敏性資料或文件，不得存放於對外開放的資訊系統中。

5、 密等以上的公文及資料，不得以電子郵件傳送；敏感性資訊如有電子郵件傳送之必要，須經加密處理後傳送。

柒、 地政人員資訊安全管理

地政人員工作職責須使用或處理資訊資源者，應依相關法令課予機密維護之責任，並加強工作考核與人員離（休）職時之權限控管。

捌、 資訊安全之通報及演練

各單位如發現系統有安全漏洞、受威脅、系統弱點及功能異常等資訊安全事件，應依相關程序立即處理，並須配合基隆市政府及行政院國家資通安全會報每年舉辦之演練作業進行演練操作。

玖、 本政策奉核定後實施，修正時亦同。