

交通部公路總局高雄區監理所

資訊安全政策

一、資訊安全政策制定

(一)目的

高雄區監理所(以下簡稱本所)為強化資訊安全管理，保護本所資訊資產，免於遭受來自於本所內部或外部以及來自人為、蓄意或意外之破壞。爰依據「行政院及所屬各機關資訊安全管理要點」、「國家機密保護法」、「智慧財產權法」及「電腦處理個人資料保護法」之相關規定，併衡酌本所業務需求，制定本所資訊安全政策，提供相關人員共同遵循。

(二)定義

資訊安全之本質為維護公路監理電腦資料的機密性、完整性及可用性。

1. 機密性(Confidentiality)：適當的劃分資訊資產的機密等級，並依其機密等級予以適當的規範及保護。
2. 完整性(Integrity)：確保各項資訊資產的完整，以期組織能正確運用該項資產。
3. 可用性(Availability)：確保各項資訊資產能提供即時且正確的服務，以滿足使用者的需求。

(三)目標

確保本所監理業務相關電腦資訊資料、系統、設備及網路之安全，避免因人為疏失、蓄意破壞或自然災害等風險，遭致資訊資產不當使用、洩漏、竄改、破壞等情事，而影響電腦作業系統正常運轉或損及民眾權益。

(四)涵蓋範圍

本資訊安全政策之範圍涵蓋下列事項：

1. 資訊安全政策制定及評估
2. 資訊安全組織及權責
3. 人員安全管理及教育訓練

4. 資訊資產之安全管理
5. 實體及環境安全管理
6. 通訊與操作管理
7. 網路安全管理
8. 系統存取控制
9. 系統發展及維護之安全管理
10. 風險評鑑與管理
11. 資訊安全事故管理
12. 業務永續運作計畫
13. 建立資通安全稽核制度及落實進行資通安全內部稽核工作

(五) 適用性

本政策所規範之事項，其適用之對象為本所編制內(外)員工、委外服務廠商及與本所連線作業之機關(構)；且涉及資訊安全管理之資產範圍者，皆有責任執行此一政策，並將獲得本所管理階層的支援。

二、資訊安全政策之評估

- (一) 本資訊安全政策，每年至少進行一次獨立及客觀的評估，以反映本所資訊安全管理政策、相關法令規範、資訊技術環境及業務之最新狀況，確保資訊安全之實務作業確實遵守資訊安全政策，且確保資訊安全實務運作之可行性及有效性。
- (二) 資訊安全政策之評估，可責由具有專業技術及知識之外部稽核單位、獨立客觀的資深主管人員，或是委請公正超然的民間專業組織或團體，進行資訊安全政策執行成果之評估。
- (三) 每年至少二次對所屬人員進行資訊系統及技術應用之安全評估，以確保其遵守資訊安全政策及規定。
 1. 應列入資訊安全評估的對象如下：
 - (1) 資訊設備及系統提供者。
 - (2) 資訊及資料擁有者。
 - (3) 使用者。
 - (4) 管理者。
 - (5) 系統維護者。
 - (6) 其他有關人員。
 2. 資訊系統擁有者應配合定期的資訊安全評估，檢討相關人員是

否遵守本資訊安全政策、規範及有關安全規定。

3. 應定期檢討及評估各項軟、硬設備的安全性，以確保其符合本資訊安全標準；評估對象應包括作業系統之評估，以確保系統軟體及硬體的安全措施，正確及有效地執行。
4. 如專業人力及經驗不足，得委請民間專業組織團體(如：外部稽核單位)協助。
5. 系統安全評估應由具有專業知識及豐富經驗的系統工程人員，於權責主管人員的監督下，以人工的方式執行，或是以自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。

(四) 資訊安全政策及規定之宣達

1. 訂定本所資訊安全作業規範，敘明人員資訊安全角色及責任的相關規定。作為執行與控管資訊安全的依據。
2. 透過公告程序，責成所屬人員瞭解本所資訊安全政策之相關規定，俾益其遵循。
3. 員工如違反資訊安全相關規定，應依紀律程序處理。

三、權責

- (一) 資訊安全小組應提供明確之指示，適時修訂本政策，以確保本政策符合需求。
- (二) 本所高階主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾，並適時覆核本政策。
- (三) 人員應透過適當程序落實本政策之要求。
- (四) 本所編制內(外)員工、委外服務廠商、所有相關資訊資產及與本所連線作業之機關(構)，皆須遵循本政策。
- (五) 本所所有相關同仁皆須應透過適當回報機制，回報所發現之資訊安全事件或弱點。
- (六) 本所所有同仁未遵循本政策或發生其他任何危及本所資訊安全之行為，將訴諸適當之懲罰程序或法律行動。
- (七) 本所所有相關同仁皆須簽署保密協議書，並瞭解於本所工作期間所取

得之資訊均為本所資產，不得使用於其他未授權之用途。

四、本資訊安全政策經本所資訊安全小組討論通過後，簽奉所長核定公布實施，修訂時亦同。

