交通部臺灣區國道高速公路局

資訊安全管理制度

ISMS-1-001

資訊安全政策

(V1.0.0)

修訂紀錄

文件版本	修訂日期	修訂者	修訂內容摘要
0.0.1	104/09/07	蘇貴丁	根據 ISO 27001:2013 及 BS 10012:2009 之要求，首次制訂。
0.1.0	104/11/10	蘇貴丁	資安管理分組審查通過
1.0.0	104/12/31	蘇貴丁	資安小組審查通過並簽核公布

目錄

壹、文件目的

本文件在律定交通部臺灣區高速公路局（以下簡稱本局）資訊安全管理制度之資訊安全政策及管理目標要求，做為本局資訊安全管理制度活動之作業準則，以確保全管理制度作業之實施，符合本局之需要及與資訊安全相關國際標準之要求。

貳、適用範圍

一、管理制度

本文件係根據本局管理之需要，並參考 ISO 27000 系列(資訊安全管理)、ISO 31000 系列(風險管理)、ISO 20000 系列(資訊技術服務管理)及 BS 10012(個人資料管理)等國際標準要求，以及中華民國政府相關國家標準、法規及行政規則所制定，以滿足 ISO 27001:2013 國際標準認證之要求。

二、組織範圍

本文件適用於本局(含所屬機關)資訊安全管理制度之規劃、實作、管理與改善。

參、政策與目標

一、資訊安全政策要求

本局之資訊安全政策，包含高階管理政策和作業層級政策二個部分，各項政策說明如下：

(一) 高階管理政策(5.1/5.3)

本局應成立跨部門之資訊安全組織，並由高階管理人員定期召開管理審查委員會議，審查本局資訊安全政策。

資訊安全組織召集人應確保資訊安全政策和目標被建立，且與本局策略方向相容。

本局之資訊安全之高階管理政策為：(5.2)
「**提升資訊服務品質、保障個人隱私、確保資通訊網路連線與資訊系統使用之安全**」。

(二) 作業層級政策

1. 移動裝置管理政策(A.6.2.1)

   所有界接到本局營運管理之網路或系統的移動裝置(包括手機、筆記型電腦、平版電腦、或其他具有儲存和連網功能之移動式裝置)，應事前經過申請與核可，始可使用。

2. 遠距工作管理政策(A.6.2.2)

   經由公眾網路(Internet)連接本局網路或系統之遠距工作，僅限連接中、低等級價值之資訊資產，且電腦應經設有本局同意之保護機制。具高等級價值資訊資產之存取，僅限於本局內部網路(Intranet)或虛擬私有網路(VPN)作業，不得直接由公眾網路連接存取。

3. 存取管制及登錄管控政策(A.9.1.1,A.9.4.2)

   界接本局網路或系統之資訊資產設備，不得設於本局外部無人看管或未具有保護機制之位置。具有存取本局資訊資產能力之設備，必須要具有唯一識別機制，且僅能由設備擁有者存取與個人工作相關之系統或資料，以便能夠監控設備存取軌跡和紀錄。擁有特別存取權限之使用者，應實施獨立監控作業，其對系統、軟體功能與資訊之存取，應經事前申請與核准，且需經過安全登錄程序管控。

4. 密碼管理政策(A.10.1.1)

   使用者之登錄密碼，須依照政府相關法規及行政規則所訂密碼最小使用長度及變更週期之要求。密碼應包含大寫字母、小寫字母、數字或特殊符號與非英文字母字元等擇三類組成，不包含使用者帳戶全名，且不得以明碼顯示。

5. 螢幕淨空政策(A.11.2.9)

   本局同仁(含借調人員及派駐人員)使用之電腦，包括伺服器、個人電腦、筆記型電腦和具有操作畫面之移動裝置，應設定電腦螢幕鎖定保護時間，且電腦在無人操作情況下，系統畫面應限時並自動進入密碼保護狀態。

6. 桌面淨空政策(A.11.2.9)

本局同仁(含借調人員及派駐人員)離開座位時，不得將機敏資料或具有足以識別個人資訊之資料置於辦公桌面，並儘可能保持桌面淨空。

7. 備份政策(A.12.3.1)

本局資訊系統與資料，依其資訊資產可用性要求，區分為高、中、低等三級。高可用性要求之資料，應執行每天備份作業；中、低可用性要求之資料，應執行每週備份作業。

8. 資訊傳送管理政策(A.13.2.1)

資訊在系統間的傳送，應在控制與保護條件下進行。在本局內部系統間傳送之資料，應在系統中設定保護機制。本局與外部組織間的資訊傳送，傳送資訊如為機敏性，傳送過程應有加密保護，且須經事前申請與核准。

9. 應用系統開發及維護政策(A.14.2.1)

自行或委外開發系統，應於系統全生命週期均將資訊安全需求納入考量。系統之維護、更新、上線執行及版本異動作業，應有安全管制措施，避免不當軟體、後門及電腦病毒等危害。

10. 紀錄保存政策(9)

本局資訊安全管理制度實施紀錄，應訂定保存年限。超過年限之紀錄，每年至少應執行一次逾時銷毀作業，並做成紀錄備查。

11. 營運持續政策

資訊化作業依業務執行之實際需求應訂定營運持續計畫，其規劃至少包含資通安全應變處理作業、事故通報處理作業及定期進行演練，務使重要系統、業務於災害發生時能於預定時間內恢復運作，以確保資訊化作業之可用性。

二、資訊安全管理目標(6.2)

本局資訊安全管理目標為：「**在合於法規、標準與契約要求條件下，確保資訊資產的機密性、完整性與可用性，防止人為疏失、蓄意或自然災害等風險因素，致資訊資產遭不當或不法使用、洩**

漏、竄改及破壞，提供持續可用、安全及順暢之系統服務」。

為達成本局資訊安全管理目標，本局參考 ISO 27001 國際標準與中華民國政府機關所公布相關法規及行政規則要求，建立本局資訊安全管理制度，對本局資訊安全管理制度實施範圍內之重要資訊資產採取適當保護措施，以維持資訊資產的機密性、完整性與可用性，使各項業務能順利且安全的執行，提供用戶優質服務。

為確保資訊安全管理制度之實施，能夠達成營運之需要，本局資訊安全管理目標，依實行之需要，展開為作業流程目標及資訊安全管理作業目標二部分。

(一) 作業流程目標

各作業流程之目標，在描述與界定各作業流程，實作資訊安全管理制度的基本要求。

(二) 資訊安全管理作業目標

資訊安全組織應每年評估與建議本局資訊安全管理作業目標，提請管理委員會議審查，包括：

1. 業務(資訊)服務可用性目標。
2. 控制業務(資訊)服務，發生資料遭不當揭露事故之管理目標。
3. 資料被竄改或未經授權存取事故之管理目標。
4. 每月機房進出管制目標。
5. 每月備份作業之管理目標。
6. 帳號密碼設定管理目標。
7. 控制安全區域經媒體揭露之資訊安全事故之管理目標。
8. 營運持續維運計畫演練之管理目標。
9. 非計畫性之營運中斷時間之管理目標。

三、資訊安全管理制度制訂與實施(6.1.3)

本局資訊安全組織應依據政策與目標之要求，制訂與維護資訊安全管理制度、推動與管理資訊安全管理制度之實施、監控與評估

資訊安全管理制度實施績效、改善資訊安全管理制度。

資訊安全組織應根據 ISO 27001 標準要求，每年審查與修訂資訊安全控制措施之適用性聲明，並提請管理委員會議審查。

肆、責任

一、本局應成立資訊安全組織，統籌管理制度相關事項之推動。

二、管理階層應積極參與及支持管理制度，並透過適當的標準和程序以實施本政策。

三、本局全體員工(含借調人員)、委外服務廠商(含派駐人員)與訪客等皆應遵守本政策。

四、本局全體員工及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

五、任何危及資訊安全與個人資訊保護之行為，將視情節輕重追究其民事、刑事及行政責任或依本局之相關規定進行議處。

伍、實施與修正

一、本政策由本局資訊安全組織定期或因應組織、業務、法規或環境等因素之變迭，予以適當修訂，經管理委員會議審查通過，陳請機關首長核定後實施，以確保本政策持續之合宜性、適切性及有效性。

二、本政策透過公告程序，使本局同仁及相關人員瞭解資訊安全政策之相關規定。