交通部公路總局

個人資料保護暨資通安全管理政策

文件制/修訂一覽表

制修訂日期	制修訂人員	制修訂版本	文件啟用/制修訂說明
105.11.18	安侯顧問	1.0	初版發行
	安侯顧問	1.1	因應各機關文件審查建議調整
	安侯顧問	1.2	因應 BS 10012 標準改版

目　錄

壹、 目的

本政策發行之目的，係藉由一份書面化文件，說明所有個人資料保護與資通安全政策(以下簡稱本政策)與管理項目（包括個資法、BS 10012、ISO 27001 國際標準及控制目標要求)，並提供相關佐證資料供查驗，做為確保本局個資保護與資訊安全管理系統運作持續順暢之依據。

貳、 範圍

一、 本政策範圍為本局及所屬各機關/單位之所有個人資料及資訊資產。

二、 適用於本局及本局業務往來之相關機關（構)、廠商及第三方機構，所涉及個人資料之蒐集、處理利用等活動。

參、 名詞定義

無

肆、 權責

一、 交通部公路總局個資、資安暨資訊服務管理組織召集人應定期審核本文件，核定後施行，修正時亦同。

二、 各機關個資暨資安管理組織應配合本文件要求辦理。

伍、 作業內容

一、 個資保護目標為符合相關法令及主管機關規範之原則，建立完善之個人資料管理制度，確保業務範圍內個人資料均妥善管理。

二、 業務範圍內有關個人資料之蒐集、處理及利用之作業流程，應防止個人資料遭受竊取、竄改、毀損、滅失、洩漏或其他不合理之利用，並善盡善良管理人之責任，以建立民眾信任基礎並維護當事人權益。

三、 本局遵循個人資料、設備安全管理程序，確保個人資料安全性，尤其未成年人之資料。

1. 未成年人之定義，依民法第 12、13 條規定，係指未滿 20 歲之無行為或限制行為能力人；依歐盟一般資料保護規則(GDPR)第八條規定，係指未滿 16 歲之兒童。

四、 本局遵循個人資料蒐集、處理及利用管理程序，確保相關作業符合法令、法規之要求及例外適用情形，依特定目的之必要範圍，於適當、相關及不過度之前提下，以最小化原則辦理，並維持資料之正確性及即時更新。

五、 制訂於法令、法規或其他適當之合法基礎允許前提下，將資料進行跨國境移轉之管理程序，管理程序應包含移轉前確認資料已經適當保護之作業方式。

六、 制訂於適當時機，向個資主管機關提出個資保護說明或提供必要文件之作業程序。

七、 制定受理當事人行使個人資料權利之處理及當事人客訴、提起法律權利及損害賠償等處理程序，尊重當事人資料查詢、閱覽、提供複製本、補充、更正、停止處理/利用、刪除、調閱等各項權利，確保公正、公平、合法、透明的資料處理方式及提供必要之資訊使當事人知悉。

八、 制定個人資料事故預防、通報及應變管理程序。

九、 定期進行個人資料管理稽核，確認管理制度運行狀況及個資相關作業所必要保存之相關紀錄、軌跡資料之完整性。

十、 持續維護及改善個人資料管理制度，確保個資管理制度正常運作。

十一、 本局遵循個人資料保護法及其施行細則，並依實務作業執行以下事項：

1. 本局應建立管理組織，界定個人資料管理相關責任及義務。

2. 透過個人資料盤點、風險管理等程序，完善本局風險管理措施。
3. 建立本局合法之個人資料蒐集、處理與利用程序等，符合個人資料保護法及其施行細則所要求之各項義務與責任。
4. 本局辦理委外作業時，應考量個人資料管理相關要求，妥善監督受託廠商，並要求遵循本管理政策及相關規定。
5. 本局應定期進行個人資料管理之內部稽核事項。
6. 本局應建立有關個人資料事故管理等相關程序。
7. 本局應重視並受理當事人就其個人資料依法行使之權利請求，並建置申訴管道、當事人提起法律權利及損害賠償之業務等處理程序。
8. 本局應持續維護及改善已建立之個人資料管理制度，包含內外部利害關係者參與管理制度運作的程度。
9. 本局應制定隱私權公告及網站隱私權聲明，內容包括有關本局對個人資料及隱私權之保護措施；網站隱私權聲明亦應公告於本局全球資訊網站。

十二、 本局及所屬各機關之個人資料保護暨資通安全政策目標訂定為「個資保護、全體動員，資通安全、人人有責」以期建立一個機密性、完整性與可用性的個資保護與資通安全環境，並達成以下目標。

(一) 「個資保護、全體動員」目標

1. 落實資訊保護政策，確實遵守資訊存取與實體環境安全管理作業程序。
2. 尊重智慧財產權，禁止安裝未經授權之電腦軟體，並對可攜式設備之使用嚴加管控。

3. 全體共同攜手動員，確保監理資料妥適安全，防止任何侵害。

(二) 「資通安全、人人有責」目標

1. 落實資通安全政策，加強資通安全教育宣導。
2. 建立資通安全量測指標，評估資通安全運作成效，落實營運持續與管理改善。
3. 嚴格遵守網路與通訊管理作業程序規定，防止各類惡意程式與電腦病毒入侵。
4. 人人遵守資訊存取控制管理作業程序規定，避免資通安全人為疏失。

十三、 本政策之執行與管理

(一) 政策執行

1. 為落實執行本政策，訂定本局各項個資及資通安全管理作業規定並「公告週知」，期能全體同仁一致遵循。
2. 為檢視本政策的執行成效，每年應由總局管理代表檢視年度目標執行成果。

(二) 政策宣達

1. 本政策節錄後，於「公路總局網站」對外公告。
2. 本政策、作業程序書、員工個資及資安作業規定與年度資通安全量測指標等文件，於「公路總局 e 化中心」上公布與宣達，供本局同仁遵循。

(三) 政策審查與評估：每年定期召開管理審查會，針對資安政策與年度量測指標的落實度加以審查與評估，以達系統持續管理改善之目的。

十四、 適用性聲明

依據 ISO 27001 國際標準及控制目標要求及本局所建立之系統文件，提出「適用性聲明書」（COMM-POL-4003）來佐證系統之完整性與可用性。

十五、 資訊安全管理系統要求

(一) 一般要求：在整體營運活動與其所面臨資通安全風險中，本局已建立、實作、運作、監視、審查、維持及改進已文件化之資訊安全管理系統。

(二) 資訊安全管理系統之建立與管理：本局依據上級主管之要求、營運特性、ISO 27001 國際標準及控制目標要求，來建立本局之資訊安全管理系統。

(三) 驗證範圍參照「適用性聲明書」（COMM-POL-4003）。

(四) 依據本局所訂定之「資訊資產清查及風險評鑑作業程序書」（ISMS-IAM-2001），評估本局本次驗證範圍內資訊資產之風險，並對結果訂定可接受之風險等級。

(五) 資訊安全管理系統實施過程中，所選擇的控制目標與控制方法，經實際運作並提出佐證資料後證明有效。

(六) 適用性聲明中所選擇不適用之控制目標，均有適當之理由。

十六、 文件管制

(一) 所建立之資訊安全管理系統文件，均依照 ISO 27001 國際標準及控制目標要求編撰對應之作業程序書、風險評估報告與風險處理計畫。

(二) 資訊安全管理系統文件之制訂、增修、審核、識別、登錄、發行、使用、存檔、作廢等作業，依照「文件與記錄管理作業程序書」（COMM-DRM-2001）之規定執行。

(三) 資訊安全管理系統所產生的報表與紀錄之編號與保存年限等，均配合前述規定進行。

十七、 管理階層責任

(一) 管理階層承諾

1. 本局管理階層承諾下列事項。
   (1) 確保個資暨資安政策已經建立。
   (2) 確保 ISO 27001 國際標準及控制目標要求均已實施。
   (3) 個資及資安管理系統之組織職掌與分工已成立並開始運作。
   (4) 本政策宣達至相關單位與人員。
   (5) 持續實施資訊資產風險管理、評估與改善。
   (6) 制（修）訂風險評估後之可接受風險值（分數）。
   (7) 提供充分資源，維持本系統持續改善與運作。
   (8) 執行本系統之管理階層審查。

(二) 資源管理

1. 資源提供
   (1) 建立、實作、運作、監控、審查、維持及改進本系統。
   (2) 確保已實施之個資及資安管理系統所有相關文件均保持其完整性與可用性。
   (3) 與承包商簽訂之契約，皆已明訂個資及資安條款。
   (4) 對所有已經實作的管控措施，提供最新的個資及資安資訊與技術持續改善。
   (5) 對本系統稽核、審查發現之缺失，優先提供改進資源。
   (6) 對任何可以改進本系統之有效性措施，提供適當改進資

源。

(三) 訓練、認知及能力：個資及資安管理系統之有關訓練、認知及能力需求等作業，依照「人力資源安全控制作業程序書」（COMM-HRM-2001）實施。

十八、 稽核

依照「內部稽核作業指導書」（COMM-IAP-3001）之規定，執行資通安全內部稽核。

十九、管理階層審查

依照「管理審查作業程序書」（COMM-OMR-2001）之規定，實施資通安全之管理階層審查。

二十、資訊安全管理系統之改進

(一) 持續改進：經由本政策執行、績效檢討、稽核實施與監控，加以分析並提出矯正與預防措施，經審查矯正與預防措施實施效果，作為持續改進本系統之依據。

(二) 矯正措施：依照「矯正預防措施作業程序書」（COMM-CPP-2001）對本政策執行、績效檢討、稽核實施與事件監控時所發現之缺失，提出矯正措施加以改善。

(三) 預防對策：依照矯正預防措施對本政策執行、績效檢討、稽核實施與監控時所發現之缺失，經改善後提出預防對策並加以規範。

陸、 參考文件

一、 適用性聲明書(COMM-POL-4003)

二、 資訊資產清查及風險評鑑作業程序書(ISMS-IAM-2001)

三、 文件與記錄管理作業程序書(COMM-DRM-2001)

四、 人力資源安全控制作業程序書(COMM-HRM-2001)

五、 內部稽核作業指導書(COMM-IAP-3001)

六、 管理審查作業程序書(COMM-OMR-2001)

七、 矯正預防措施作業程序書(COMM-CPP-2001)

柒、 附件

一、 個人資料隱私權宣告與聲明(COMM-POL-4001)

二、 線上隱私權聲明(COMM-POL-4002)

三、 適用性聲明書(COMM-POL-4003)