交通部公路總局臺中區監理所資訊安全管理作業規範

交通部公路總局臺中區監理所 98.09.03 中監資字第 0981006797 號函修正
交通部公路總局臺中區監理所 99.7.30 中監資字第 0991006042 號函修正
版本：第 4 版修訂版

壹、總則

一、依據：

電腦處理個人資料保護法、國家機密資料保護法、政風機構辦理資訊使用管理稽核作業要點與行政院暨所屬各機關資訊安全管理規範辦理。

二、目的：

為確保本所監理業務電腦資訊資料、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，特訂頒本作業規範。

三、適用對象

（一）、人員

本所員工及使用本所資訊資源或業務委外服務之廠商人員等。

（二）、應用系統

二代公路監理系統、行政管理系統、網際網路應用系統等。

（三）、硬體設備

各式主機、工作站、伺服器及個人電腦等。

（四）、網路及其他設施

本所辦公室之區域網路，公路監理系統網路、網際網路之數據專線及相關網路設施。

貳、組織與權責

一、資訊安全管理組織

為統籌本所資訊安全管理事宜，應成立本所「資訊安全處理小組」（以下簡稱本小組），由技術副所長擔任召集人，政風室、資訊室及各業務單位（電腦管理員）組成，共同負責本所資訊安全管理工作。

二、權責分工

（一）、本所年度公務機密檢查及資訊安全之稽核，由政風室會同相關單位負責辦理。

（二）、資訊系統安全控制技術事宜由資訊室負責辦理。

（三）、資料及資訊系統之安全使用及保護事宜，由各業務單位負責辦理。

叁、規範內容

一、人員安全與管理

(一)、人員安全管理

1、本所新進人員於報到時，需簽署保密切結書。保密切結書涵蓋期間包括從業期間與離職後，均有保密之責任，任何因未遵守本資訊安全管理規範導致之資訊安全意外事件將依相關規定懲處。

2、本所資訊業務委外服務之廠商人員，應於簽訂契約同時簽署保密切結遵守資訊安全管理規範。

3、本所員工離職或調任其他單位時，需依照人事室規定填寫離職單，並由資訊室撤銷帳號核章後，始完成離職手續。

4、電腦使用者如因職務異動而成為非授權使用者時，相關單位應主動通知資訊室系統管理人員撤銷該使用者帳號。

(二)、教育訓練

1、本所新進人員應由業務單位施以適當的系統操作訓練，避免使用者不當操作。

2、新系統上線時，應對其作業人員、維護人員及網路管理人員施以適當的教育訓練。

3、對本所員工辦理資訊安全管理訓練課程，提昇其危機意識與資訊安全概念。課程中必須給予完整之軟體著作權與版權觀念，嚴禁使用非法軟體，自由軟體（freeware）與共享軟體（shareware）之安裝使用亦必須詳細了解並遵守其版權宣告。

4、每年度應針對所內資訊人員辦理或參加上級或其他機關辦理之資訊安全管理危機處理防護課程訓練。

5、應隨時注意資通安全最新訊息，參與資通安全相關訓練，並利用內部網路公布本所員工知悉。

6、每年度應由政風室對員工施以電腦處理個人資料保護法、國家機密資料保護法及相關法令等之宣導、訓練或講習，提醒法治觀念。

二、電腦系統安全管理

(一) 監理系統安全管理

1、資料檔案處理參照中華電信數據分公司編印各項監理業務電腦系統文件、交通部或公路總局各級主管單位相關規定及本所各項業務電腦系統相關規定辦理。

2、停電或電腦故障時即依公路總局訂頒交通部公路總局各監理所、站、分站停電或電腦故障監理業務緊急應變作業流程處理。

3、電腦系統作業時程(如 cronfile)的設定，由系統管理人員負責管制，遇有新增及更動時，並知會相關單位或相關人員。

4、電腦系統及資料庫管理員之 root 及 informix 密碼，應定期(每三個月)或可能外洩時予以更換。

5、系統及應用程式每一個月執行一次備份，以確保系統資料的安全。

6、遇有系統作業技術問題，應即向電腦管理員申告處理，如未能解決再由電腦管理員聯繫本所資訊室處理。

7、其他單位外界系統欲與本所公路監理電腦系統連線或互傳資料時，均需陳

報公路總局，並以公路監理電腦系統中央資訊中心為統一對外之窗口。

（二）資料安全管理

1、電腦資料鍵入、異動須依據各系統作業操作手冊，及其他相關規定辦理。
2、電腦操作員應確實核對報表，發現錯誤即時更正，主管課股長(或指派專人)應不定期抽查稽核。
3、發現電腦資料錯誤且無法經由終端機鍵入更正時，應填寫資料異動聯繫單，陳單位主管核准後，送交或傳真資訊室執行更正，資訊室相關系統負責人將更正步驟內容及時間記錄於聯繫單並保存備查，傳真之資料異動聯繫單應保存備查。
4、資料庫每日應執行一次備份，以確保資料的安全。
5、處理含個人資料時應依據「電腦處理個人資料保護法」及相關規定審慎處理，不私自蒐集或洩漏業務機密，非公務用途嚴禁調閱使用。
6、提供治安、情治機關相關資料應依據公路總局訂定之「交通部公路總局所屬監理單位提供情治情報機關車籍資料作業要點」規定辦理。
7、其他單位索取資料應有正式公文，業務單位提供治安情報機關相關資料應依據「電腦處理個人資料保護法」及相關規定予以審查，並簽奉核准後始可提供資料。
8、駕駛人或車輛所有人申請查詢或請求閱覽其個人資料或製給複製本時，應填寫申請書；如申請之資料已登載於駕駛執照、行車執照、拖車使用證及牌照登記書者，應請其依相關規定辦理申請。
9、個人申請提供他人車籍資料時，應持有債權憑證；持法院判決書裁定書或支付命令確定證明書等，應填寫申請書，由業務單位發函逕提供資料於法院。

(三)、電腦病毒及惡意軟體之防範

1、電腦防護軟體及系統回復軟體由資訊室統一進行定期規劃評估與建置安裝。
2、本所員工應統一使用合法版權軟體，避免上網下載來路不明之軟體
3、與外部交換資料時，使用資料前應啟動病毒防護軟體偵測。
4、本所員工應隨時更新病毒碼並下載修補系統漏洞。
5、本所員工操作電腦系統如發現病毒時應立即清除，並通報資訊室病毒或惡意程式名稱。無法清除病毒時應通知資訊室派員協助處理。

(四)、日常作業之安全管理

有關日常作業之「資料備份」、「系統錯誤事項之處理」及「電腦作業環境之監測」等事項均應遵循「交通部公路總局監理業務電腦化作業手冊」及「公路監理資訊資料庫備援制度」規定，確實執行，以維持業務之正常運作。

(五)、電腦媒體之安全管理

1、應納入管理的電腦媒體包括儲存公務上應保密資料之可移動的磁帶、磁碟、光碟及其他儲存裝置、電腦列印之各式報表、作業程序目錄級系統文件等。
2、機密性之資料若需使用傳真設備傳送時，傳真設備必須有保護措施，避免資料外洩。
3、電腦媒體應依保存規定要求，存放在安全環境，非經簽奉所（站）長核准，

不得攜離辦公場所。

4、媒體儲存的資料，不再繼續使用或逾保存年限時，應將儲存內容刪除；報廢時應由專人以安全方式（例如燒毀、以碎紙機處理或將資料從媒體中完全清除）處理。

5、電腦媒體運送過程，應有妥善之安全措施，以防止資料遭竄改破壞、誤用或未經授權使用。

6、電腦媒體運送，應慎選安全及可信賴的運送機構或人員，對於機密及敏感性的資料應採取特別的安全保護措施，必要時得加派人員運送。

三、網路安全管理

（一）、網路安全管理與規劃

1、應設專人管理網路系統，維持網路（含備援設備）系統正常運作。

2、屬開放性網路系統應具有防火牆功能及安裝入侵偵測、防毒系統，以防止非法入侵破壞網路。

3、網路系統管理人員應負責製發帳號，提供取得授權人員使用；除特殊情況並簽奉所（站）長核准外，不得製發匿名或多人共享的帳號。

4、網路系統管理人員應負責監督網路資料使用情形，檢查有無違反資訊安全規定事件發生。

（二）、網路使用者管理

1、本所員工經申請帳號後成為合法授權的網路使用者，並在授權範圍內存取網路資源。

2、為防杜電腦資料因下載 P2P 軟體後發生洩密情事，使用者不得使用 P2P（peer-to-peer）檔案分享程式、抓檔軟體、續傳軟體等或利用電子郵件服務進行任何可能對網路的正常傳輸造成的不利影響行為。

3、為防止即時通訊系統(Instant Messaging Systems)被濫用，並降低資訊安全風險及頻寬成本，本所員工有需使用即時通訊系統需求者，應敘明理由提出申請，經首長或其授權代理人同意後，始得安裝及使用即時通訊系統，並由資訊室處理後續之權限設定及管制作業；本所員工使用即時通訊系統，應避免作為私人用途，並嚴禁討論及傳輸機密及敏感性資料。
本要點所稱即時通訊系統，指使用者透過網際網路，和特定對象以語音、文字、影像或檔案進行互動溝通之軟體工具，包含 Yahoo!Messenger 、MSN Messenger、AIM （ AOL ） American OnlineInstant Messenger、ICQ（I Seek You）及其他目的及效果相近之軟體。但不包括資訊室統一建置功能相近之同類軟體。

4、本所網路使用者應遵循以下規定：

(1)、不得將自己的登入身分識別帳號與密碼交付他人使用。

(2)、不得使用他人的登入身分識別帳號與密碼

(3)、非經授權禁止以儀器設備或軟體工具讀取網路上的通訊資料。

(4)、禁止下載未經授權使用的檔案或軟體。

(5)、禁止將色情檔案建置在本所網路，亦不得在網路上散播不法、不當或違反善良風俗習慣之資料。

(6)、禁止利用本所網路從事不法、不當之情事。

(7)、不得散佈電腦病毒或以其他任何手段蓄意或妨害網路系統的正常運作。

(三)、電子郵件安全管理

1、電子郵件收送依據本所網路郵局（webmail.tmv.gov.tw）服務條款辦理，並由專人負責每天定時收送電子郵件，必要時得隨時收送電子郵件。

2、敏感性資料經加密作業處理得以電子郵件傳送；機密等以上公文及資料，不得以電子郵件傳送。

3、來路不明的電子郵件，不宜隨意打開，以免啟動惡意執行檔（病毒檔），使網路系統遭到破壞。

4、禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量郵件。

(四)、網際網路應用之安全管理

1、本所電腦使用的電腦，應安裝防毒軟體，以對下載的檔案作病毒掃描。

2、應在瀏覽器上自訂安全等級，並採取適當安全防護措施防止網際網路上的應用程式任意更改檔案系統，以維護內部網路安全。

3、應考量網際網路新技術可能安全弱點，並採取適當的防護措施以確保內部網路安全。

(五)、網路入侵處理

1、發現網路入侵之處理步驟

網路使用者發現網路入侵之情事實應立即通知資訊室，資訊室接獲通知後，應採取下述適當措施以防止災害繼續擴大：

(1)、當確定本所網路安全被突破時，被入侵之應用系統應暫時設定為「拒絕任何存取」，並切斷入侵者連接，如無法切斷則必須關閉網路連接。

(2)、應正式記錄入侵的情形及評估影響的層面。

(3)、如入侵者已被資訊室嚴密監控，再不危害內部網路安全的前提下，得適度有條件地允許入侵者存取動作，以利追查入侵者。一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。

(4)、立即向權責主管人員報告入侵情形。

(5)、依資安事件通報應變機制通報。

(6)、向機關內部或外部之電腦緊急處理小組反應，以獲取必要之協助。

2、網路入侵之追蹤調查

(1)、檢視紀錄檔中是否有不尋常的來源位置或不尋常的操作動作。檢查登入時間、程序的執行紀錄與系統日誌所做的紀錄等以防止入侵者修改紀錄檔來隱藏行蹤。

(2)、對入侵者的追查，除利用稽核檔案提供外，得使用系統執行反向查詢，並聯合相關單位追蹤入侵者。

(3)、當檢查機器是否被入侵時，必須檢查所有區域網路上的機器。如一台機器被入侵，同一網段的其他機器也可能已被入侵；或是入侵者利用其他機器為窗口入侵本所網路。

3、網路入侵的事後處理

(1)、入侵者的行為若觸犯法律規定，構成犯罪事實，由政風室查處，並立即告知警調單位，請其處理入侵者之犯罪事實調查。

(2)、資訊室應全面檢討網路安全及修正防火牆的設定，尋求適當的解決辦法，以防禦類似的入侵與攻擊。

(六)、網路安全稽核

1、網路系統管理人員應不定時檢視系統登錄紀錄，並視需要產生報表。如發現異常狀況應立即通報單位主管，情節重大時應專案簽報並知會政風室。

2、應視需要建立警示系統，讓網路系統管理人員在特定的網路安全事件發生時，及時獲得警示性的信號，俾利採取有效的防範措施，減少網路安全事件的發生。

四、系統存取控制

(一)、應依執行業務之需求，視個案逐項考量賦與使用者系統存取權限；系統存取權限之配賦，應以執行業務及職務所必要者為限。

(二)、應用系統操作人員均各自擁有自己的使用者代碼和密碼，不同的使用者代碼各有不同的作業範圍和權限，密碼必須加以保密，避免洩密遭人盜用，並應定期更改通行密碼。

(三)、使用者代碼新增、刪除或修正作業範圍和權限，應填寫終端機操作人員使用者代碼異動聯繫單，陳單位主管核備後，由資訊室或各站之電腦管理員執行管制。並定期於資訊業務稽核時，依聯繫單進行抽查檢視。

(四)、使用人員領取使用者代碼後應立即自行設定密碼，密碼長度最少應由六位長度組成；如遺忘密碼應填寫終端機操作人員使用者代碼異動聯繫單，由機房電腦管理員清除密碼後，再由操作人員自行設定密碼。

(五)、終端機操作人員離職，人事單位應知會資訊室或電腦管理員，其原屬單位應填寫終端機操作人員使用者代碼異動聯繫單，陳單位主管核備後，由資訊室或各站之電腦管理員立即撤銷其使用權限。

(六)、閒置不用的識別碼不應重新配賦給其他的使用者，並應不定期實施稽核。

(七)、人員因故離開座位暫停作業時，必須登出系統或使用畫面鎖定保護，防止帳號被盜用或被竊取。下班或公出離開辦公室前，必須關閉電腦設備，避免有心人士竊取機密資料或入侵系統。

(八)、使用者代碼(識別碼、電腦帳號)與使用者系統存取權限每年應定期清查一次。

五、資訊資產之安全管理

(一)、建立資訊系統有關資訊資產目錄，明列資訊資產的項目、管理(負責)人及安全等級分類，如有變更應詳細記載。

(二)、機關資訊安全分類依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，區分為機密性、敏感性及一般性等三類。

(三)、資訊資產實體設備故障應通知資訊資產管理(負責) 人，並由管理(負責)人依規定提出請修申請，並登錄設備故障月報表及送修進出時間表。

(四)、資訊資產實體設備報廢，由財產管理人員依規定辦理。

(五)、含儲存媒體的設備，應在報廢處理前詳加檢查，以確保機密性、敏感性之資料及有版權的軟體已被移除。

六、系統發展與維護安全管理

（一）、公路監理電腦系統

1、公路監理電腦由中華電信數據通信分公司統一開發與維護。

2、應用系統程式之更新，由資訊室各應用系統負責人員配合中華電信數據通信分公司執行。

3、因應業務需求之系統功能新增或異動，應由需求單 位填寫業務聯繫單，由單位主管核可後，送資訊室處理；惟如涉及全國一致性之作業需求，業務單位應循行政體系陳報公路總局核可後，再轉中華電信數據通信分公司配合辦理。

（二）、行政電腦系統

1、本所一般行政業務電腦化系統由公路總局統一開發與維護。

2、應用系統程式之更新，由資訊室各應用系統負責人員配合公路總局執行。

3、因應業務需求，應由業務單位提出計劃書，資訊室得視人力、技術、成本及資訊安全考量提出可行性方案及意見（或辦理情形）回復原需求單位。

（三）、委外作業安全管理

1、資訊業務委外時，應於事前審慎評估可能的潛在安全風險，並與廠商簽訂適當的資訊安全協定，及課以相關的安全管理責任，納入契約條款，必要時不定期派員監督、管理委外廠商實際作業情形，並保有稽核權利。

2、委外作業承包之工作人員，如需進入相關系統作業，由委外業務之主管單位依規定申請使用者代碼，並於委外業務完成後立刻依規定撤銷。

3、委外作業鍵入之資料，由主管單位指派專人核對，以確保資料之正確性。

4、系統委外開發，承包商應提供系統建置（含規格及軟體程式）之完整、詳細說明文件。

5、自行管理的設備應安置在特定區域，並與資訊服務提供者管理的設備分開。

七、實體及環境安全管理

（一）、電腦設備安全管理

1、專人負責管理，每年應定期檢核各項設備安全，並加以記錄。

2、定期維護保養，確保設備的完整性及可以持續使用。

3、電腦設備、資料或軟體，未經管理人員同意並登錄資訊資產外借登記簿或電腦終端設備送修登記簿，不得攜離辦公處所。

（二）、電源供應系統的管理

1、相關電腦設備之電源使用應依據製造廠商提供規格設置、並須防止斷電或電力不正常導致的傷害。

2、緊急供電系統暨不斷電系統應由專人負責管理及制定開關機操作程序，並定期維護保養及測試。

3、謹慎使用電腦延長線，避免電力無法負荷導致火災等危害安全事情。

4、電腦專用電源除電腦相關設備外，其他任何電器均不得使用。

（三）、電腦機房消防系統的設置管理

1、專人負責。

2、定期維護保養及測試，確保設備的完整性及可以持續使用。

3、電腦機房消防安全緊急處理作業程序以書面記載，並定期演練及測試。

（四）、其它安全管理

1、電腦機房實施門禁安全控管。
2、資訊支援或維護服務人員須由資訊室人員或電腦管理員陪同或是被授權並經登記，始得進出管制區域。
3、備援媒體應存放在安全距離以外之地點。
4、個人電腦及終端機不使用時，應關閉結束作業或設定鎖定螢幕等控制措施保護。
5、嚴禁安裝或下載未經授權使用或來路不明之軟體。
6、電腦機房及各項電腦軟硬體設備應強化設（放）置處、所防護措施，避免遭致水患、風災、火災等災害，造成損失。

八、業務永續運作計劃之規劃與管理

（一）、備援與回復作業

1、本所公路監理資訊系統及資料庫之備援（備分）及復原作業，應遵循交通部公路總局訂頒之監理業務電腦化作業手冊「檔案與資料管理」及「公路監理資訊資料庫備援制度」之規定，確實執行，以維持業務之持續運作。
2、個人電腦中之重要資料備份應由同仁定期自行進行備份，並應選擇乾燥密閉之環境保管備份媒體。
3、監理電腦系統遇有停電、線路或機件故障、或重大天然災害時，應遵循交通部公路總局訂頒之監理業務電腦化作業手冊「監理電腦作業停電、故障緊急處置實施要點」、「交通部公路總局各區監理所、站、分站停電或電腦故障監理業務緊急應變作業流程」之規定，作妥善之應變處置。
4、每年應進行資訊安全風險評估及作業檢討，並據以修正本所「資訊安全管理作業規範」，以確保資訊安全實務作業之有效性。
5、每年應進行備援、回復作業程式機制之測試演練。

（二）、資訊安全事件通報處理機制

1、本所業務如因資訊安全事件（包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，相關人員應視其狀況嚴重程度及影響層面，循序向各權責主管報告。
2、本所員工發現有資訊安全事件時，應迅速通報各權責主管單位及人員處理。
3、資訊室相關人員接獲通報後應紀錄相關的訊息，並應依『行政院資通安全危機通報及應變作業計劃』規定向上通報。
4、資訊室相關人員應立即停止使用受影響之電腦系統或設備，並保留現況。
5、系統管理人員處理後，應向直屬業務主管回報處理結果，並作成紀錄。

九、資訊安全稽核

（一）、資訊機密維護及稽核使用管理事項，由政風室會同資訊室及相關單位組成安全稽核小組負責辦理，併得並本所公務機密維護檢查辦理。
（二）、稽核之結果應填寫紀錄表完整記錄。
（三）、資訊安全稽核結果，除特殊原因得簽奉核可不公開外，應彙整相關單位之優缺點及綜合改進建議，簽奉核可後提供相關單位改進。

（四）、安全稽核小組因應突發性、專案性或特殊性之資訊安全稽核需要，得不定期針對特定目的之項目、單位或人員進行資訊安全專案稽核工作。

（五）、專案稽核之重點以因應特殊目的為主，稽核內容則因審視稽核項目是否已按規定辦理。

（六）、專案稽核之結果，應即時檢討各項優缺點及綜合改進建議，簽奉核可後提供相關單位改進，並列入下年度稽核時追蹤。

肆、附則

一、 本所員工、使用本資訊資源及委外服務人員違反本規範之作業規定者，得視情節輕重，由有關單位依相關規定予以處分，或依法追究其民、刑事責任。

二、 本規範如有未盡事宜，得隨時修正。

三、 本規範未定之事項得依行政院所頒定之「行政院所屬各機關資訊安全管理規範」及相關之規定辦理。

四、本規範經簽奉所長後實施，修正時亦同。

資訊安全管理作業規範文件更新紀錄表

日期	版次	更 新 內 容 說 明	核准者	備 註
93.5.10	00	新訂	陳所長增義	93.05.10 中監資字第 0930019929 號函訂定
94.11.17	01	叁、規範內容 二、電腦系統安全（四）、日常作業之安全管理 修正“有關日常作業之「資料備份」、「系統錯誤事項之處理」及「電腦作業環境之監測」	陳所長增義	94.11.17 中監資字第 0940018980 號函修正
97.7.29	02	修正”叁、規範內容 三、網路安全管理（二）、網路使用者管理增加”2.不得使用 P2P…”	陳所長增義	97.7.29 中監資字第 0971006357 號函修正
98.8.31	03	1.修正”叁.規範內容/三.網路安全管理/(二)網路使用者管理 3.加入”為防止禁止即時通軟體. ”” 2.修正”叁.規範內容/六、系統發展與維護安全管理/(二)委外作業安全管理 1.加入”…保有稽核權利 ””	陳所長聰乾	98.9.2 中監資字第 0981006797 號函修正
99.7.26	04	叁、規範內容四、系統存取控制（八）、使用者代碼（識別碼、電腦帳號）與使用者系統存取權限每年應定期清查一次，或於必要時清查。	陳所長聰乾	99.7.30 中監資字第 0991006042 號函修正