政府資料傳輸平臺管理規範

一、 數位發展部(以下簡稱本部)為提升跨機關資料安全傳輸服務機制，以政府骨幹網路(GSN)為基礎，建立政府資料傳輸平臺(以下簡稱 T-Road)，並確保各機關在 T-Road 上資料傳輸之資訊安全及隱私保護，特訂定本管理規範。

二、 本管理規範之適用對象為政府機關，不包括國營事業、教育部所屬各級學校、國防部及其所屬機關(構)、醫療機構。

三、 T-Road 包括資料傳輸功能管理平臺(以下簡稱 T-Road 管理平臺)及安控伺服器，T-Road 管理平臺包括下列各子系統之運作：

(一)中央控管系統(Central Server System)：負責各安控伺服器之憑證管理、登錄註冊、各機關提供之資料、各項異動即時通知等。

(二)設定管理服務(Configuration Management)：管理各安控伺服器組態之下載及更新。

(三)運作監控服務(Operational Monitoring)：紀錄、蒐集、彙整各安控伺服器及 T-Road 管理平臺之操作紀錄，並保存相關查調紀錄。

(四)環境監控服務(Environmental Monitoring)：紀錄、蒐集各安控伺服器及 T-Road 管理平臺之環境使用及運作狀態，並依狀況啟動相關備援機制。

(五)時戳服務(Time Stamp Service)：提供 T-Road 資料傳輸服務任何紀錄之時戳證明，確保紀錄之完整性、不可否認性。

(六)紀錄查調服務 (Query Platform Service)：提供機關查詢異動紀錄及傳輸紀錄。

(七)單一簽入服務(Single Sign On)：提供身分識別機制以確定使用者之身分。

四、 本管理規範用詞，定義如下：

(一)T-Road 維運機關：指本部，負責 T-Road 各項功能開發及 T-Road 管理平臺維運。

(二)資料中心設置機關：指依行政院及所屬各機關資料中心設置作業要點之規定，設置資料中心之機關。

(三)介接機關：指申請透過 T-Road 傳輸資料之機關，包括資料需求機關及資料提供機關。

(四)資料需求機關：指介接及透過 T-Road，取得資料提供機關傳輸之資料，辦理線上服務之機關。

(五)資料提供機關：指介接及透過 T-Road，提供資料需求機關辦理線上服務所需資料之機關。

(六)安控伺服器(Security Server)：本部開發具安全傳輸資料功能，用以介

接 T-Road 進行點對點資料傳輸之伺服器。

(七)應用程式介面服務(以下簡稱 API 服務)：指基於應用程式介面(Application Programming Interface, API)技術規格所提供之資料傳輸服務。

五、 申請介接 T-Road 之機關，應由資料中心設置機關向本部提出申請並辦理下列事項：

(一)申請 T-Road 專屬之政府網際服務網虛擬私有網路(以下簡稱 GSN VPN)網路。

(二)申請資料傳輸專屬網域，網域命名原則：機關名稱縮寫.troad.gov.tw。

(三)申請安裝 T-Road 專屬類伺服器應用軟體憑證。

(四)架設安控伺服器及該安控伺服器環境之規劃與管理，並確保該安控伺服器與其他機關安控伺服器連線之實體及運作環境之安全。

(五)安控伺服器應架設於資料傳輸網段，並與外部服務網段及內部服務網段進行區隔，提高資料傳輸安全。

介接機關將介接 T-Road 之申請書上傳至中央控管系統網頁申請，經 T-Road 維運機關核可者，以該安控伺服器介接至 T-Road。

六、 介接 T-Road 之網路環境設置，應符合下列規定：

(一)介接機關應使用 GSN VPN 或經本部核可之安全連線方式介接 T-Road。

(二)介接機關應採專屬之資料傳輸網段進行 T-Road 資料傳輸作業，該資料傳輸網段不得連線外部服務網段。

(三)介接機關以內部服務網段與 T-Road 資料傳輸網段連線者，應採限制 IP 及點對點之連線方式。

(四)介接機關應評估傳輸之資料量，提供資料傳輸服務順暢運作所必要之網路頻寬。

(五)T-Road 內虛擬私有網路 IP 位址，由本部以資料中心設置機關為單位統一配發。

(六)資料中心設置機關應依本部規劃之 IP 及網域命名原則，建置其所屬機關之網路環境。

七、 介接機關之安控伺服器應具備身分驗證功能，其操作者及經授權使用人員應通過身分驗證後，始得使用之。

介接機關以其他資通系統介接安控伺服器者，應自行提供該資通系統之身分驗證功能，其授權使用人員應通過身分驗證後，始得使用之。

前二項之身分驗證紀錄，介接機關應至少保存五年，並應配合資料提供機關之查核。

八、 透過 T-Road 資料傳輸前，應確認該資料傳輸符合資通安全管理法、個人資料保護法、本管理規範及該介接機關所定資料傳輸規定等相關法令規定。

九、 透過 T-Road 傳輸資料者，應先由資料提供機關於其安控伺服器辦理 API 服

務之註冊，該 API 服務由 T-Road 管理平臺同步至其他機關安控伺服器。

前項註冊之 API 服務，其服務名稱及描述等欄位應具意義且易於識別，並符合共通性應用程式介面規範之規定。介接機關應透過安控伺服器提供或取得 API 服務。

前項服務管理之使用權限，由資料提供機關設定之；該機關並得就資料需求機關資料保管及服務使用之紀錄，進行查核。

十、 資料提供機關與資料需求機關應以書面共同協議傳輸內容，由資料需求機關將該協議之證明文件上傳至安控伺服器，資料提供機關應於確認後開啟服務存取權限。

資料需求機關之資通系統應符合資通安全責任等級分級辦法所定資通系統防護基準之要求。

十一、透過 T-Road 傳輸之資料為檔案者，應以安全檔案傳輸方式進行；為 API 訊息者，所傳輸之訊息均應有數位簽章。

介接機關就提供或取得之資料，應依法令負保密之責；就該資料之完整性及正確性，並應自行負責。

資料需求機關就所取得資料為申請目的以外之利用，屬個人資料者，依個人資料保護法之規定辦理；非屬個人資料者，應經資料提供機關事前同意。

資料需求機關就取得且暫存於安控伺服器之檔案，應於使用目的完成後，予以刪除；其保留期間不得逾七日。

資料需求機關應控管已取得資料之安全；資料提供機關得視需要，就資料需求機關取得資料後之管理進行稽核。

十二、介接機關終止介接或暫停介接者，應以安控伺服器建立之終止或暫停介接功能進行，並於預定終止或暫停日一個月前，以函文通知相關機關。

十三、安控伺服器稽核日誌之保存，應符合下列規定：

(一) 應完整保存 T-Road 資料傳輸產生之稽核日誌，包括資料傳輸紀錄、設定異動紀錄等。

(二) 稽核日誌應有數位簽章及時間戳記保護。

(三) 稽核日誌應異機保存至少五年。

(四) 應定期檢視稽核日誌之完整性及有效性。

(五) 稽核日誌應同步上傳至 T-Road 管理平臺備查。

十四、本部負責 T-Road 之維運，應辦理下列事項：

(一)T-Road 傳輸服務整體功能之規劃與開發、障礙排除與異常處理、訂定管理規範、T-Road 傳輸資料機密性、可用性及完整性驗證機制之設計。

(二)T-Road 整體系統與網路、安控伺服器效能與服務可用性之監測。

(三)發布最新安控伺服器清單、API 服務清單及其授權狀態至各機關安控伺服器。

(四)各安控伺服器稽核日誌之蒐集，必要時，其紀錄應提供作為追蹤軌跡

及查證用。

十五、資料中心設置機關應依下列規定，維護安控伺服器及辦理相關事項：

(一)視資料傳輸需求及效能，評估其本機關及所屬機關安控伺服器之安裝數量、位置、硬體規格及備援環境。

(二)評估及安裝本部提供之安控伺服器軟體。

(三)向政府憑證管理中心申請安控伺服器所需憑證並安裝，且定期檢視該憑證效期。

(四)安控伺服器應專機專用，不得安裝非必要軟體；並應以防火牆或其他安全設施，管控該伺服器與其他主機間之資料傳輸。

(五)安控伺服器禁止與網際網路連線。

(六)各安控伺服器間之資料傳輸，應透過政府憑證管理中心核發之 TLS 憑證進行雙向驗證及通道加密。

(七)偵測發現惡意程式或發生資安事件時，應先行阻絕資料傳輸，避免蔓延至其他機關，並追查惡意程式來源，通報 T-Road 維運機關及相關機關。

(八)應配合開啟 T-Road 管理平臺各系統與安控伺服器間之連線，及控管所應使用之通訊埠。

十六、介接機關，應辦理下列事項：

(一) 管理安控伺服器作業系統及軟體環境，確保該安控伺服器服務可用性。

(二) 配合 T-Road 管理平臺所發布之安控伺服器作業系統或軟體安全性更新通知，於七日內完成更新。

(三) 安裝安控伺服器之防毒軟體，並定期更新病毒碼，確認透過 T-Road 傳輸之資料無感染病毒。

十七、資通安全管理作業，依下列規定辦理：

(一)T-Road 維運機關、資料中心設置機關及介接機關，應依資通安全管理法及個人資料保護法等相關法令規定，辦理安全維護措施，並落實資通系統委外安全管理。但介接機關有更嚴格之資通安全管理規定者，從其規定。

(二)資料中心設置機關應將 T-Road 相關之資通系統及設備，納入其資訊安全監控中心(SOC)之監控範圍；偵測發現傳輸有異常流量者，應轉知 GSN SOC。

(三)資料中心設置機關及介接機關發生 T-Road 傳輸之資安事件者，應依資通安全事件通報及應變辦法之規定進行通報，並通知 T-Road 維運機關。

十八、T-Road 維運機關應定期或不定期對介接機關進行監督及查核，其範圍應包括介接安控伺服器之資通系統。經發現有異常狀況者，T-Road 維運機關得要求限期提出說明或改善措施，介接機關應配合辦理之。

T-Road 維運機關發現介接機關有阻擋 T-Road 相關管理功能，或違反本管

理規範之規定者，得通知其限期改善，屆期未改善或情節嚴重無法改善者，終止或暫停其介接 T-Road。

經依前項規定終止或暫停介接 T-Road，而其情節得改善者，應於完成改善後，始得重新申請介接。

十九、本管理規範未盡事宜，依本部相關操作手冊或公告辦理。

二十、第二點所定非屬本管理規範之適用對象，確有介接 T-Road 之需要，且專案申請經本部同意者，得準用本管理規範之規定。