

# 桃園市政府資通系統開發及維運安全作業原則

中華民國 113 年 6 月 17 日府智安字第 1130148846 號函頒訂

- 一、桃園市政府（以下簡稱本府）為積極推動資通安全政策，確保本府及所屬各機關系統開發、維護之安全及正常運作需要，特訂定本原則。
- 二、原則適用對象為本府及所屬各級機關（以下稱各機關）。
- 三、本原則用詞定義如下：
  - （一）資訊系統：泛指由軟體（套裝程式、應用程式、系統軟體及行動應用軟體等）、硬體（個人電腦、伺服器及行動裝置等）、資料、程式和人員所組成，旨在收集、處理、儲存和傳遞資訊，以支援組織內部之運作及決策。
  - （二）系統開發：泛指為達成特定目的，採用程式語言及硬體設備，創造及實現新軟體或資訊系統過程。
- 四、資訊系統開發過程，開發框架以使用者為中心考量，並依政府數位服務指引，提供主動服務為內涵，達成簡化服務流程、提升服務效能、創新使用體驗為目標，並考量後續維運財務規劃，作為評估自行或委外開發及訂定優先順序之發展原則。
- 五、開發系統前，應優先評估是否已有共通性系統可以使用，並以鼓勵民間運用本府開放資料平台(Open Data)或共通性應用程式介面(Open API)進行增值開發為原則，擴大民眾參與並降低開發維運成本。同時評估運用響應式網頁設計(RWD)及漸進式網路應用程式(PWA)替代行動應用軟體(App)所提供之操作介面。
- 六、開發資訊系統時，應依資通安全管理法及子法與個人資料保護法要求加密敏感資料，在資料傳輸和存儲過程中嚴格保護隱私。
- 七、系統軟體、資料庫或作業系統最高權限帳號，應由機關人員保管，不得授與委外廠商使用；廠商使用測試或維護帳號等，應依資通安全維護計畫以及資訊安全管理系統(ISMS)文件辦理。
- 八、各機關設置之資訊系統或網站應向本府智慧城鄉發展委員會(以下簡稱智發會)提出網址申請，並以配發網址對外公開，不得直接以 IP 位址或其他未被許可之網域為其網址，網址規定如下：
  - （一）機關入口網站，原則應以\*.tycg.gov.tw 網域為其網址；如原有網址以為\*.gov.tw，則以\*.gov.tw 網域為其網址。
  - （二）機關入口網站以外之其他系統或網站，應考量必要性而以\*.com 為其網址；智發會得要求機關說明。
  - （三）各機關申請 IP 及防火牆設置需配合智發會資訊安全管理系統(ISMS)填寫使用申請單。
- 九、各機關設置之資訊系統應建立完善資通安全事件應變計畫，於發生資安事件時，及時回報智發會，並依其指示以降低損失和影響。

- 十、資訊系統設置應依資通安全責任等級分級辦法評定系統安全等級，按資通系統防護基準要求辦理，並依國家資通安全研究院訂定之資安服務需求建議書範本，將相關要求納入委外開發契約。本府及所屬各機關應定期檢討系統安全分級，確保資訊系統分級妥適性，並依資訊系統分級辦理風險評鑑及執行防護基準。
- 十一、資訊系統維運環境應配合導入政府組態基準（GCB）、資通安全弱點通報系統(VANS)及端點偵測及應變機制(EDR)政策，以降低成為駭客入侵管道機率。
- 十二、開發網頁型服務應依數位發展部政府網站營運交流平台之政府網站服務管理規範辦理，每年接受智發會考核，並依數位發展部政府網站即時檢核系統之評分結果進行優化，以提升網站服務品質。
- 十三、系統開發建置或功能擴增經費分析，依據政府資訊服務採購經費估算編列手冊，各機關得視個案情況或發包策略調整計畫成本，並得整併項目以簡化預算內容，惟仍須核實考量所需費用，避免重複編列或遺漏。
- 十四、各機關辦理資訊系統開發時，應評估系統維運需要，於開發契約訂定保固服務及範圍，並於保固期滿後始得編列維護費用。本府及所屬各機關於編列預算時，應依據本府預算編列原則及數位發展部訂定之資通系統籌獲各階段資安強化措施指引，單獨列出资安經費，以達到資安防護目的。
- 十五、各機關辦理資訊系統開發或維運時，如無法依本原則之規定辦理，應敘明原因及擬採行之資安作為，並經機關資安長同意後辦理。
- 十六、開發資訊系統時，應依政府數位服務指引，資通安全管理法、身心障礙者權益保障法、著作權法及個人資料保護法等規定辦理，並採用安全軟體發展生命週期(SSDLC)執行。
- 十七、各機關針對資訊安全管理應依 CNS/ISO 27001 規定辦理，於 SSDLC 模型設計及開發階段，訂定安全設計和開發標準，包括但不限於安全編碼標準、資安組態標準等；在 SSDLC 模型之測試階段，應進行安全測試和驗證，包括但不限於原始碼審查、漏洞掃描、安全測試等。
- 十八、各機關之資訊系統完成建置後，應辦理下列事項：
  - (一) 建立完整系統備份及還原計畫，並依資通系統防護基準，每年至少進行一次實際演練操作。
  - (二) 建立持續監控和改進機制，每年至少一次檢查和評估系統之安全性，並經複測後，依檢測結果改進資訊安全管理制度及措施；如有委外廠商之系統維護情形，亦應配合定期稽核或以其他檢測方式進行監控和改進。
  - (三) 配合本府或中央主管機關進行定期或不定期技術性檢測(弱點掃描及滲透測試)，並具備弱點或漏洞修補能力，於修補完成後依限回報檢測機關。
- 十九、各機關應提供資訊安全培訓及定期舉辦資訊安全活動，促進所屬人

員對資訊安全之重視。

二十、各機關應依資通安全管理法導入資訊安全管理系統(ISMS)，並符合其所屬資通安全責任等級之要求。

二十一、其他資訊系統服務管理事項及安全作業規範應依數位發展部訂定之政府網站服務管理規範、網站無障礙規範及資通安全管理法規定辦理。

二十二、各機關係統伺服器安裝於本府資訊機房時，應配合智發會訂定之電腦機房及設備安全維護作業說明書與實體及環境安全管理程序書辦理；安裝於各機關自建機房時，網路安全措施由機房管理單位負責。如租用廠商機房或雲端服務時，相關資訊安全或管理責任由租用機關負責。

二十三、各機關對所屬人員依本原則辦理，具重大績效或缺失者，得依桃園市政府及所屬各機關學校人員資通安全事項獎懲基準簽報行政獎勵或予以懲處。

二十四、有關本府資訊機房管理及資訊安全所需表單由智發會定之。