南投縣資訊系統開發及維運作業要點

一、　南投縣政府（以下簡稱本府）為確保系統開發、維護之安全與正常運作，特訂定本作業要點以為依循。

二、　資訊系統應依「資訊系統分級與資安防護基準作業規定」評定系統安全等級，並依資安防護基準之要求進行開發，或參考「資訊系統委外開發RFP 資安需求範本」將相關要求得納入委外開發契約。

三、　系統程式開發上，應配合政府組態基準（Government Configuration Baseline，GCB）政策，以降低成為駭客入侵管道，有關政府組態基準相關政策資訊，請參考行政院國家資通安全會報技術服務中心(http://www.icst.org.tw/GCBIntro.aspx)相關準則辦理。

四、　網頁程式設計開發上，應避免可能存在的安全弱點，相關準則得 參 照 行 政 院 國 家 資 通 安 全 會 報 技 術 服 務 中 心 (www.nccst.nat.gov.tw/CommonSpecification)之共通規範-Web 應用程式安全參考指引。

五、　系統開發與維運等業務經評估後，採委外開發或維運時，除應遵守本府資安相關規範外，下列基本原則應考量納入服務建議書或合約：

(一)承包廠商應繳交「需求規格書」、「設計規格書」、「系統安裝及維護手冊」、「系統測試報告」、「系統備份及還原計畫」、「系統原始碼光碟」、「軟體使用授權文件(若有)」及「系統執行檔光碟(若有)」等資料，並至少提供一份電子檔，交由承辦單位確實點收並妥善列入移交。承商應控管交付之系統與文件版本一致。

(二)資安漏洞檢測及修正：為確保所開發系統之資料安全性與完整性，提供系統之 SQL Injection、XSS(Cross-Site Scripting)、惡意程式碼（如病毒、蠕蟲、特洛伊木馬、後門程式、間諜軟體等）及隱秘通道（covert channel）之測試報告，同時修正程式可能之漏洞或保證無惡意程式碼（需提供完整測試報告及修正結果報告）。

(三)智慧財產權之歸屬（開發後軟體所有權）。

(四)相關保密合約、事件發生處理與處罰條款。

(五)系統建置完成後，系統維護的責任與方式。

(六)明訂各項服務水準含服務內容、服務項目、技術能力、叫修時間、回復時間、廠商的支援配合、解決問題的能力及實行資訊安全的能

力等。

六、 本府得視需要為瞭解委外廠商資安防護現況，實施資安稽核並據以要求廠商配合改善，其改善期間視危害程度在必要時，本府得中斷系統連線或關閉系統運作。

七、 系統於完成建置後需提供完整之系統備份與還原計畫，必要時配合本府進行實際演練操作，以確認相關機制確實可行。

八、 系統於完成建置後，本府及中央單位將不定期進行弱點掃描及滲透測試，各系統管理單位應具備弱點或漏洞修補能力，並於修補完成後回報測試單位。

九、 各資訊系統應定期檢討其安全分級，以確保資訊系統分級妥適性，以利辦理風險評鑑及執行防護基準。

十、 系統、軟體或作業系統最高權限帳號、資料庫最高權限帳號，應由本府人員保管，不得直接授與委外廠商使用。承商使用之測試或維護帳號等，應依本府相關申請規定辦理。

十一、 委外廠商履行合約應提供其使用之軟體，且須為合法軟體，並不得違反智慧財產權之規定，如有違反事情發生，委外廠商須承擔所有法律責任。

十二、 本府暨所屬機關得視本身業務或管理之需求，依據本要點另訂相關規範或程序書施行。