臺南市政府111年度資訊安全內部稽核
自我檢查表

使用說明:本表用於協助本府使用電腦設備人員(含駐點廠商與當日在場之委外人員)，於查核期間進行自我檢查相關資安配合事項(註)。

單位:　　科別：　　姓名：　　分機:

適用人員	自我檢查項目	請依據日期進行查核與確認		
		自行檢查	複檢結果	備註
所有人員	1. 人員是否了解資訊安全宣言? 安全、正確、迅速	☐	☐	☐
所有人員	2. 個人螢幕保護程式是否已啓動？a.時間設定為15分鐘以內 b.密碼保護打勾	☐	☐	☐
所有人員	3. 登入個人主機或伺服器之密碼長度是否符合八(含)個字元以上？	☐	☐	☐
所有人員	4. 是否定期三個月變更密碼？	☐	☐	☐
所有人員	5. 密碼之設定是否符合複雜度之規範？大小寫、英文數字混合或特殊字元。	☐	☐	☐
所有人員	6. 機敏性及限制性資訊（紙本類含呈核公文）是否已有機密等級標示	☐	☐	☐
所有人員	7. 確認個人所保護（管）之機密性資料(含文件、報表及磁帶媒體等)是否已妥善保存？a.是否放置於上鎖的櫃子 b.是否應放置於特定場所	☐	☐	☐ 個人隨身碟是不可棄置桌面，須放在上鎖抽屜
所有人員	8. 是否已建置防毒軟體？a.防毒程式是否啟動 b.病毒碼是否更新	☐	☐	☐免費、付費、wni10內建均可
所有人員	9. 確認是否有跟他人使用共同帳號？若有，應提出個別帳號之申請。	☐	☐	☐ 電腦登入名稱不可為user, admin, administrator, root…等
所有人員	10. 確認執行資安相關業務的紙本文件得保留三年，電子紀錄檔須保	☐	☐	☐

	存三年			
所有人員	11. 是否了解資安事件通報的程序？a.何種事件需要通報－電腦當機及中斷服務、惡意的程式碼、阻斷服務、業務資料不完整，或是資料不正確導致的作業錯誤、機密性資料遭侵犯、資訊系統的不當使用、其他影響資訊業務事件 b.通報對象－資安事件通報受理人員	☐	☐	☐
所有人員	12. 個人是否安裝合法軟體，非經核准，不可安裝非公務用軟體，包括即時通訊軟體如 Line、Whatsapp、Wechat、Skype 等？a.個人合法之軟體確認是否可以在府內使用？ b.若無法確認是否為合法使用之軟體，請於驗證時暫行移除	☐	☐	☐ 個人電腦安裝之軟體須經過合法授權；電腦內軟體應識別是否為公務使用
所有人員	13. 確認已移除不必要或危害國家資通安全疑慮之資訊與通訊設備	☐	☐	☐
所有人員	14. 下班後員工是否將經辦之機密性或敏感性資料，妥善收藏?	☐	☐	☐
所有人員	15. 設備報廢前是否將機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫?	☐	☐	☐
所有人員	16. 設備報廢後如確定不再使用時，是否將儲存之資料及軟體移除後並做實體破壞?	☐	☐	☐
所有人員	17. 資訊資產如須攜出場外使用，是否均經事前授權，並作安全查核?	☐	☐	☐
所有人員	18. 棄置之手寫或影印公文廢紙及已過保存期限之公文，若為機密性、敏感性者是否予以銷毀?	☐	☐	☐影印廢紙不可存在公務資料或出現單位名稱
所有人員	19. 是否定期對電腦系統及資料儲存	☐	☐	☐

	媒體進行本機病毒掃描?			
所有人員	20. 所有電腦鐘訊是否定期核對校正?以確保時間記錄正確。	☐	☐	☐
所有人員	21. 郵件收信軟體有無關閉預覽功能及使用純文字讀取信件。	☐	☐	☐檢查對象為資訊服務入口網信箱
所有人員	22. 個人資料保護及管理是否設有專人及知悉保護程序	☐	☐	☐
所有人員	23. 單位是否設有專人負責軟體授權管理及定期辦理盤點，相關資料備有軟體目錄及軟體保管清單？	☐	☐	☐
所有人員	24. 個人電腦名稱是否依規定命名(PC+分機號碼)？	☐	☐	☐
所有人員	25. 作業系統及相關資訊軟體是否即時更新?	☐	☐	☐
系統管理員	26. 是否建立有帳號管理機制？ a.是否有閒置帳號 b.是否有非授權使用者(含異動與離職者) c.確認定期（半年）所產出之管理報表有定期審查並給予意見簽核	☐	☐	☐ 市府稽核受檢系統是否進行帳號清查
系統管理員	27. 是否設置有遠端連線，若設有遠端連線是否經過申請？遠端連線時，確認主控端是否勾選下列項目？ a.連線加密選項 b.啟動 logs 稽核日誌	☐	☐	☐
系統管理員	28. 是否有建立及啟動系統查詢軌跡紀錄檔(Log)，並保留六個月之紀錄，以作為日後調查及監督之用。	☐	☐	☐市府稽核受檢系統是否啟用 log 記錄功能並保留6月
系統管理員	29. 系統紀錄檔，是否有定期備份轉出檔案後保存。	☐	☐	☐市府稽核受檢系統 log 是否納入備份

系統管理員	30. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用自建之失敗驗證機制。	□	□	□市府稽核受檢系統是否啟用帳號登入失敗鎖定機制
系統管理員	31. 是否建立資安事件時通報機制且定期通報政風單位。	□	□	□
系統管理員	32. 是否執行弱點掃描安全檢測，並且有修補紀錄。	□	□	□
系統管理員	33. 確認所管理之資訊資產皆已納入資產清冊且進行風險評鑑？ a.若為關鍵性資產得適時加入 b.非重要資產則請於半年內加入	□	□	□
系統管理員	34. 是否隨手將機房門禁確實關閉？	□	□	□
系統管理員	35. 資訊委外作業，是否明定廠商之資訊安全責任？ a.廠商保密切結書 b.資訊安全責任條款或要求 C.是否有規劃或執行委外廠商稽核	□	□	□
系統管理員	36. 是否維持機房溫度24±4度 相對溼度維持在30%RH 至60%RH	□	□	□
系統管理員	37. 日誌內容是否包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊。	□	□	□市府稽核受檢系統 log 內容是否包含左列資訊
系統管理員	38. 資通系統是否使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間 (GMT)。	□	□	□市府稽核受檢系統是否對時時間伺服器
系統管理員	39. 是否執行系統源碼與資料備份，並且有異機或異地備份。	□	□	□市府稽核受檢系統是否異機備份
系統	40. 資通系統是否具備唯一識別及鑑	□	□	□

管理員	別機關使用者(或代表機關使用者行為之程序)之功能。			
系統管理員	41. 使用預設密碼登入系統時，是否於登入後要求立即變更。	☐	☐	☐

註：

一、 本府各單位一般人員需針對項目1-25進行檢查

二、 本府各單位自行控管系統之管理者需針對項目1-41進行檢查