稽核日期：　　年　　月　　日

附件3

臺南市政府教育局暨所屬機關學校
114年度資訊安全內部稽核檢查表

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	檢查項目及重點	請依據日期進行查核與確認		
		自行檢查	複查結果	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。 c.防毒軟體啟動自動掃描。	□	□	
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。	□	□	
所有人員	9.是否了解個資與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	□	□	

	料不完整或外洩、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、個人資料外流與其他影響資訊業務或個人權益的事件。 b.通報對象－資安事件通報資安專責人員/資安窗口；個資外洩事件通報個資窗口。			
所有人員	10.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。			
所有人員	11.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	12.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	13.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	14.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	15.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？	□	□	
所有人員	16.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	17.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	18.郵件收信軟體有無關閉預覽功能及使用	□	□	

人員	純文字讀取信件。			
所有人員	19.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	20.個人電腦名稱依規定命名(PC(2碼)+地點(2碼)+單位別(3碼)+分機(4碼)+英文流水號(1碼))。	□	□	
所有人員	21.作業系統及相關資訊軟體即時更新。(例如 windows、Java、Adobe Reader、7-zip)。	□	□	
所有人員	22.是否針對共用區(如 NAS)中有關個資法第2條第1項所稱之個人資料等機敏性資料加密保存？	□	□	
所有人員	23.個人電腦桌面所存放之資料，是否包含個資法第2條第1項所稱之個人資料？若有，是否進行加密保護？	□	□	
所有人員	24.公務往來傳輸之郵件是否包含個資法第2條第1項之個人資料？若有，是否對附件檔案壓縮加密後再行傳輸？	□	□	
所有人員	25. 不使用公務使用之電子郵件註冊於非公務外部網站或外部服務。	□	□	
所有人員	26. 機關總部電腦導入以下軟體。 a.B 級以上機關：VANS 及 EDR/MDR。 b.C 級機關：VANS	□	□	
所有人員	27. 請問貴單位過去一年點擊社交工程電子郵件同仁，已參加講習。	□	□	
所有人員	28.如有使用危害國家資通安全產品應列冊管理及汰換時程規劃。	□	□	
系統管理員	29.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。			
系統管理員	30.遠端連線應經過申請或特定 IP 通過。	□	□	
系統管理員	31.應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。	□	□	
系統管理員	32.系統紀錄檔，應定期備份轉出檔案後保以及應異機備份。	□	□	
系統管理員	33.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。	□	□	
系統管理員	34.發生資安事件結案應會辦政風單位。	□	□	
系統管理員	35.是否確認資通系統相關漏洞修復之狀態。	□	□	
系統管理員	36.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	37.是否隨手將機房門禁確實關閉？	□	□	
系統管理員	38.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.廠商違約處罰條款。	□	□	
系統管理員	39.是否維持機房溫度約24度？ 相對溼度維持在30%RH 至60%RH。	□	□	

系統管理員	40.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。	□	□	
系統管理員	41.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)。	□	□	
系統管理員	42.是否執行系統源碼與資料備份，並且有異機或異地備份。	□	□	
系統管理員	43.資通系統是否具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能。	□	□	
系統管理員	44.使用預設密碼登入系統時，是否於登入後要求立即變更。	□	□	
系統管理員	45.是否落實執行資通安全管理法施行細則第4條第1項第9款規定，資訊系統委外作業，機關定期以稽核或其他適當方式確認廠商作業之執行情形？	□	□	
系統管理員	46.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。	□	□	
系統管理員	47.網頁及對外系統應具備因應惡意攻擊之緩解機制(如：阻擋 IP、靜態頁)。	□	□	
系統管理員	48.如有所屬機關，應定期監督所屬機關執行資通安全維護計畫實施情形。	□	□	
系統管理員	49.單位如保有電子防疫個資，應履行個資宣告，特定目的消失後應立即刪除，並保留刪除佐證資料。	□	□	

【備註】：

一、本局各單位一般人員需針對項目1-25進行檢查

二、本局各單位自行控管系統之管理者需針對項目26-46進行檢查