網路零售業資安基本查核表說明(草案)

網路零售業資安基本查核表(以下簡稱本表)係為經濟部商業司委託財團法人資訊工業策進會制定，並由中華民國無店面零售商業同業公會負責推動網路零售者(以下簡稱業者)資安基本防護自主管理，以引導業者建立資訊安全防護。

一、目的：

本表旨在提供業者以資安基本防護基礎進行個資安全防護管理，協助業者因應法規要求，落實個資安全防護。本表屬於鼓勵業者建立自主管理，建議業者可參考本查核表，但不以此為限，並考量業者營運風險與需求，訂定符合業者本身營運需求之個資安全防護管理。

二、使用對象：

國內經營網際網路零售業及網際網路零售服務平台業。

三、如何使用本表：

本表係依據經濟部商業司於 104 年 9 月頒佈之「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」(網址：http://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040100100006900-1040917)，之規定，依序展開資安基本防護的控制措施，並分類為人員、作業、技術及設備等四大類，共四十項控制措施，並提供作業建議及應注意事項。

本表應由業者指派主管、資訊及資安相關人員，共同填寫本表。

填寫步驟如下：

(1) 依序由第一項至最後一項 (即 1 至 40 題)，以本表之建議控制措施為基準，比對業者本身現行資安防護控制措施作法，將比對後之結果作為自評判斷之依據，擇一勾選符合程度(「符合」/「部分符合」/「不符合」/「其他」)欄位，查檢結果若有後續協助需求，請在「是否需 EC-CERT 後續諮詢服務」欄位打勾。

(2) 填寫說明如下：

第 5 項次之 建議控制措施	符合	部分符合	不符合	其他	是否需 諮詢服務
員工和廠商人員，在被允許存取資訊處理設施之前，均應簽署機密性或保密協議。	符合建議控制措施作業說明第 1、2 點，請打∨	只符合建議控制措施作業說明第 1 或第 2 點，請打∨	建議控制措施作業說明第 1、2 點均不符合，請打∨	其他因素或作法說明，請打∨	需後續諮詢服務，請打∨

本表填寫後，請回傳至中華民國無店面零售商業同業公會(e-mail:nemos@cnra.org.tw)。

(3) 在「是否需諮詢服務」欄位打勾，將由無店面公會及 EC-CERT 技術團隊主動聯絡業者，提供相關諮詢。

網路零售業資安基本查核表(草案)

公司名稱：　　查核人員簽名：　　查核日期：105 年　　月　　日

類別	項次	符合	部分符合	不符合	其他	備註	是否需諮詢服務
人員	1						
	2						
	3						
	4						
	5						
作業	6						
	7						
	8						
	9						
	10						
	11						
	12						
	13						
	14						
	15						
	16						
	17						
	18						
	19						
	20						

類別	項次	符合	部分符合	不符合	其他	備註	是否需諮詢服務
作業	21						
	22						
	23						
	24						
	25						
技術	26						
	27						
	28						
	29						
	30						
	31						
	32						
	33						
	34						
	35						
設備	36						
	37						
	38						
	39						
	40						

網路零售業資安基本查核項目(草案)

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
人員	1	指定專人，負責資安及個資保護政策、計畫與管理之工作事項，並訂定相關程序文件。	§3-3	(1)正式對內部發佈人令，指派資訊主管或營業主管負責推動資安及個資保護之工作，包括識別公司適用法令法規及委外作業之聯繫與處理。 (2)資安及個資保護之政策或手冊文件其對內部發佈(公告或 mail)，向員工及廠商說明要求遵守。(政策或手冊內容包含營運作業要求、資訊安全要求事項及委外契約要求)
	2	檢查同仁存取關鍵服務、客戶資訊，客戶要求等要求內容，都已訂定各自負責之安全管理責任並正式授權實施。	§12-1	(1)檢查所有公司人員之職責，針對公司之重要服務流程，建立相互勾稽之流程，避免選手兼裁判之職責授權。如甲受理接單，則由乙審核訂單、再由丙出貨，同時甲乙丙之帳號權限及負責作業之內容不一樣。 (2)處理個資檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重新設定密碼外，應視需要更換使用者帳號。 (3)交易契約及網站等內容，都依據法令法規辦理 。如個資告知事項、資安措施及配合作業等等。
	3	每年至少執行一次公司員工資訊安全及個資保護認知宣導訓練。	§16-1/ §16-2 §19-10	(1)訂定公司年度訓練計畫，條列那些人要接受訓練?訓練課程是什麼?訓練時間? (2)每年對公司所有員工至少執行一次資訊安全及個資保護認知宣導訓練。 (3)每年應對公司指定之專人及資安人員至少執行一次資訊安全及個資保護之專業教育訓練。
	4	每年應對公司指定之專人及資安人員至少執行一次資訊安全及個資保護教育訓練。	§3-4 §16-1 §16-3	

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
			§19-10	(4)教育訓練後要考試測試，提升員工資安及個資保護之重視。 (5)教育訓練可自行安排或如參加 EC-CERT 提供的資安教育訓練課程或其他專業資安與個資保護課程。
	5	員工和廠商在獲許存取資訊或設施之前，均應簽署機密性或保密協議。	§12-4	(1)員工和委外廠商在人員報到或服務合約簽署時，應簽署機密性或保密協議書，如切結書、軟體使用規定、網際網路使用規定等。 (2)所有紀錄要留存備查。
作業	6	依據營運要求，訂定「個人資料保護管理」、「資訊安全政策」、「個人資料檔案安全維護計畫」及「業務終止後個人資料處理方法」等管理程序文件及管制措施並定期審查檢討。	§3-1/§3-2 §5-1-3 §6-1/§7-1 §9-1/§11-1 §15-1 §7-1/§18-1 §19-2-3 §20-1-2	(1)資安及個資保護政策制定與修改必須由公司的高階主管宣布，並讓員工瞭解規定內容，及公司注重之態度。 (2)至少每年一次，由公司的高階主管召開會議，於會議審查檢討文件內容及管制措施的效果並提出改善建議。 (3)對個資或機敏檔案之資訊安全處理原則與程序，應至少涵蓋下列內容： (a) 檔案於人員個人電腦或工作桌面之暫存或儲存或複製。 (b) 檔案於人員個人電腦或工作桌面之刪除或銷毀。 (c) 檔案進行內外部傳送時之資料加密或書面彌封。 (d) 可攜式儲存裝置(包括 USB 隨身碟、行動硬碟、手持媒體及通信設備等) 之使用限制與管理。 (e) 保有檔案之儲存與備份。 (f) 保有檔案之刪除與銷毀。 (g) 保有檔案之內外部傳送。 (h) 保有檔案之處理紀錄管理。
	7	客戶之個人資料及客戶交易檔案，每年至少執行一次清	§6-2/§6-3 §6-4	(1)建立資料或個資檔案之盤查及審議之管理程序。 (2)每年由高階主管及相關人員共同查核檢討一次。

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		查工作並定期審查維護。		⑶ 查核檢討若不符合管理程序，則需通知主管，立即處理改善並加強訓練。
	8	建立帳號管理，包含帳號權限之申請、異動修改、停用及刪除並定期清查帳號權限，不得有共用帳號之行為。	§12-2/§12-3 §15-2 §19-7	(1)建立帳號權限之申請、異動修改、停用及刪除之管理程序。 (2)每半年由高階主管及相關人員共同檢查帳號權限，並將帳號權限列冊管理。 (3)帳號不能多人共同使用(二個以上之人員，使用同一帳號)，若一定要用則要有其他保護措施，如值勤表或使用登記表等輔助。 (4)非負責處理個資之人員，不得具有存取或查閱個資之權限。
	9	硬體設備、應用軟體及系統軟體等之最高權限帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，並保留稽核及審查紀錄。	§12-2/§12-3 §15-2 §19-7	(1)針對網路設備、防火牆、系統、程序及資料庫管理者(含設定參數)之特權帳號權限，建立申請修改及刪除之管理程序且其帳號權限需通過主管核准。如主機系統、資料庫及防火牆等管理員之帳號。 (2)將所有的特權帳號權限列冊管理，並每半年由高階主管及相關人員共同查核檢討一次。 (3)所有特權帳號權限之申請修改及刪除之紀錄要留存備查。 ⑷ 所有的帳號之存取使用紀錄，要留存至少三個月並每季審查，若不符規定則通知主管，並立即處理、改善及加強訓練。
	10	超過所規定之預期閒置時間或使用期限，系統應自動將使用者登出。	§15-1	當使用者登入系統後，若於 15 分鐘內沒有任何作業或訊息交換，則系統即需主動將其登出強制離線。
	11	資訊系統管理者應保存可識別存取來源的稽核軌跡，並定期審查使用者帳號活動，	§15-2	(1)建立應用系統使用權限管理程序，如申請帳號及使用方法、權限設定方法等。 (2)留置使用者之使用紀錄，內容要有何人帳號/何時登入及登出時間

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		若發現帳號不正常使用時，應回報管理者及主管。		/IP 或設備名稱位置/存取資訊或使用功能等使用資源。如紀錄甲員工利用 ast1 帳號在 105/4/4 10：00 am 使用 192.168.1.20 之 host1 電腦，使用 ERP 系統查詢訂單 A0001。 (3) 應用系統使用者之使用紀錄，要留存一段時間並定期審查，若不符規定則通知主管，並立即處理、改善及加強訓練。如留存三個月並每季審查。
	12	避免使用未經授權之電腦程式，及其他可能涉及侵害智慧財產權之行為。	§15-3	(1) 不要使用沒有版權之非法軟體。 (2) 使用免費自由軟體，要檢查來源是否安全並經防毒軟體掃瞄是否安全。
	13	建立並遵循電子郵件使用安全管理作業之規定。	§15-1	(1) 建立電子郵件使用管理程序，如申請帳號及使用方法、設定電子郵件密碼長度及如何保護電子郵件等。 (2) 執行安全檢查作業，如每季作社交工程(即利用假電子郵件，測試使用者之安全認知是否落實)，若不符規定則立即改善並加強訓練。如員工使用電子郵件必須完全了解社交工程攻擊，不得輕易開啟附檔。
	14	建立並遵循使用者通行碼管理之作業規定	§15-1	(1) 建立密碼管理程序，如檢查及使用方法、設定密碼長度、設定密碼強度、多久變更一次及如何保護密碼等。如要求密碼必須謹慎使用，不得告知其他人、每 90 天必須更換一次密碼(例 105/4/1 設定密碼，則於 105/6/30 必須強制更換密碼) 、密碼長度要 8 碼以上並英數字符號大小寫等混合(例密碼 Wec12345$)。 (2) 執行安全檢查作業，如每月作 PC 之安全檢查，若不符規定則立即改善並加強訓練。
	15	個人電腦及主機應安裝具備	§15-3	(1) 個人電腦及主機裝設防毒軟體並設定自動更新病毒程式碼。

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		即時掃描及攔阻病毒之防毒軟體，並隨時更新病毒程式碼。		(2)建立防毒軟體管理程序，如檢查及使用方法、不得移除等。 (3)規定每週定期對電腦(含 PC/主機/筆電)和儲存媒體執行防毒掃瞄檢查。
	16	定期進行設備、系統元件、資料庫系統及軟體漏洞修補。	§15-3	對使用中之設備、系統元件、資料庫系統、作業系統及工具軟體等漏洞，進行自動更新修補作業，如WINDOWS/ADOBE/OFFICE/MYSQL/MSSQL/ORACLE/CISCO/JAVA/.NET/防火牆…等軟體更新。
	17	建立並遵循媒體及可攜式儲存媒體使用安全管理作業規定。	§13-1	(1)建立媒體及可攜式儲存媒體使用管理程序，如磁帶/USB/燒錄機/隨身硬碟/記憶卡等設備之開放權限原則及查核機制。如公司只能使用公司專屬式可攜式儲存媒體，不得私自攜帶使用。 (2)機密性資料，若存放於媒體或可攜式儲存媒體上，應該使用加密技術保護資料，如檔案用密碼保護後再儲存至 USB。
	18	資訊系統及設備僅開啟必要之網路、服務、程式及通道，使用者僅能存取已被授權使用之網路、服務、程式及通道。	§14-2 §15-1	(1)建立網路連線管理程序，如網路連線權限之申請、異動修改及刪除等要求。 (2)建立網路連線之安全需要規定，如網站網路連線服務只能由 80 通道(80 port)進出，其餘通道關閉。
	19	使用遠端連線應使用強度足夠之加密通訊協定，不得將通行碼紀錄於工具軟體內。	§13-4 §15-1	(1)建立遠端連線之管理程序。如使用何種協定連線交換資料?遠端權限之申請、異動修改及刪除等要求。 (2)使用 VPN/HTTPS 設備或 SFTP 通訊協定連線交換資料。 (3)帳號密碼不得儲存於系統或工具軟體內。
	20	資訊系統、個人資料、重要資料(資料庫)及軟體應定期	§13-5 §19-6	(1)每日備份最好，至少每週要備份一次，備份檔案保存三週。 (2)備份資料要檢查是否正確成功。

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		備份,並定期執行回復測試。		(3)備份檔案要離線、異地儲放。
	21	確立與營運所在地之警察機關、主管機關及 EC-CERT 等相關機構之聯絡體制、資安事件管理文件及紀錄留存。	§8-1-5 §19-8	(1)建立發生狀況時的通知管理程序，如通知誰?如何通知 ?時限為何? 等等。如發生事故時，發現人要在 2 小時內電話通知課長及經理，經理要立即通知總經理。 (2)建立發生狀況時的處理作業管理程序，如誰作何事? 如何執行 ?如何回應?如發現人要現場處理，課長及經理要支援或通知廠商及 EC-CERT 協助或向警方報案。 (3)相關作為製作成紀錄並留存備查。
	22	服務或設備委外時，應事先明確訂定作業目標、範圍及雙方權力義務。	§11-1 §13-2	(1)避免允許系統服務廠商以遠端登入方式進行牽涉個資或機密的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密方式進行（如：HTTPS、SSH 等）。 (2)雙方定期審查服務作業績效之管理監督。如每月召開服務檢討會議，討論風險狀況、事件狀況及服務指標等 (3)檢視處理作業委外合約或其他正式文件內容，需至少包括下列要求： (a) 乙方應建立個資保護及資訊安全政策，並遵循甲方的個資保護及資訊安全要求政策。 (b) 明訂甲乙雙方個資及資安之職責與工作項目及溝通方式。 (c) 乙方及其服務人員應簽署之保密承諾。 (d) 乙方應對個資保護及資訊安全之處理作業人員進行相關教育訓練 (如應在 XX 月 XX 日前，至少受過 X 小時的個資管理與安全維護訓練課程)。 (e) 乙方欲將受託之處理服務作業再進行轉包，應事先取得甲方
	23	確定委外廠商之各項安全措施可以符合資料安全及個人資訊保護等法令法規。	§11-1 §13-2	
	24	委託契約內容應包含資訊處理方式、安全政策保護及個人資料保護相關事項之管理及檢核。	§11-1	

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
				之正式許可。 (f) 乙方欲將受託之處理服務作業再進行轉包，丙方亦應符合乙方應符合之合約條款、個資管理程序及安全維護要求。 (g) 當契約終止時,相關之個資及作業資料應被銷毀或交還甲方。 (h) 規範履約過程中，甲方可適時監督與稽核乙方之相關作業(包括進行考核測試、現場稽核、教育訓練，或其他可行之監督方式等)。 (i) 倘因乙方違反個人資料保護法而遭任何其他第三人向委託機構主張任何權利、請求、索賠或訴訟等，除因甲方之故意或重大過失行為所致者外，乙方同意補償並確保甲方(包括甲方人員)不遭受亦不負擔任何索賠、責任、費用及損失。
	25	定期稽核及審查責任範圍內的資訊設施與安全政策、標準及其他任何安全要求的遵循性，並保留相關紀錄。	§7-3 §18-1-4 §19-11-12	將所有的資安及個資之防護措施彙整並至各單位評估執行狀況，並每半年由高階主管及相關人員共同查核檢討一次評估結果，相關紀錄並留存備查。
技術	26	機敏性資訊傳輸過程得採取資訊加密保護措施，資料傳送以業務所需之最少資料為原則。	§13-3 §13-4	(1) 資料在網路傳輸與儲存必須加密。如網站傳輸採取 HTTPS 之保護措施，讓網路通訊資料加密，變成亂碼。 (2) 網站資料或資料庫加密之保護措施，讓資料加密，變成亂碼。如資料利用 zip 加密、或 OFFICE 之密碼加密、資料庫可利用工具或程式設定進行加密。 (3) 要傳輸或儲存之資料欄位內容，以可以完成服務之必要資料即可。如傳輸或留存資料內有出生年月日，以作為未來生日禮之行銷用時，只需要利用月日就可，不要利用出生年。
	27	採取具備資訊隱密性功能與識別、確認對方端末設備及防止儲存資料外洩等資料保護措施。	§13-3 §13-4	

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
				(4) 雙方連線時，應利用帳號密碼及動態密碼或鎖定網路 IP 位置作身分及設備之確認。 (5) 動態密碼可使用簡訊、電子郵件或硬體式設備(Token)提供。
	28	明訂網際網路作業相關管理辦法、作業規範及網路系統安全政策，並定期檢視修訂。	§13-4 §15-1	(1) 訂定網際網路作業使用管理程序，例如：如何申請上網權限? 要安裝何種軟體及設定才可上網? 那些網站不可用? 及網際網路使用之安全要求等。如公司內網對外使用網際網路之人員管理。 (2) 使用管理程序要有審議檢查之控制。如公司使用網際網路之使用率。
	29	建立網路安全架構，於電子商務網站服務網段(主機區)建立防火牆或路由器設備，區隔外網區、DMZ 區以及內網區，並遵循防火牆安全管理程序規定。	§13-4	(1) 利用防火牆或路由器設備，將網路區分為外網與內網。外網給客戶使用，內網給公司同仁使用。 (2) 外網的通路，要管制。如誰可以連線?用什麼方式連線。 (3) 外網與內網之間的通路，要管制。如誰可以內到外連線?誰可以外到內連線?用什麼方式連線。 (4) 訂定外網與內網使用管制程序。如連線申請單。
	30	至少每年實施 1 次弱點掃描，並完成缺失改善。	§15-3	(1) 針對主機、設備及 PC，每年實施 1 次弱點掃描(1 次 2 循環)。 (2) 弱點掃描作業後會出報告(1 循環)，報告之問題，要改善，改善後再作一次弱點掃描(2 循環)。 (3) 報告要視為機密文件，妥善保管。
	31	應避免採用已停止弱點修補或更新之系統軟體與應用軟體。若一定要採用，則應採用其他配套防護措施。	§15-3	(1) 不要使用不被原廠支援的作業系統如 Windows XP / WINDOWS SERVER 2000 /WINDOWS SERVER 2003 等，原廠已停止服務之軟體。若非用不可，則採取不可上網之隔離保護。 (2) 相關軟體要隨時至原廠更新。
	32	應管制個資檔案透過輸出入	§15-5	(1) 管制 USB/FAX/MAIL/印表機/FB/LINE 等設施之使用權限申請管

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		裝置、通訊軟體、系統操作複製至網頁、網路檔案或列印等方式傳輸，並應留存相關紀錄軌跡與數位證據。	§19-1 §19-5 §19-9	理或利用工具管制權限。 (2) 對連線存取紀錄，應定期查核檢討，若有異常應立即通報主管處理，立即改善並加強訓練，如每季查核檢討一次。
	33	限制外部網路存取功能，同時外部網路可以存取的機器設備應維持在最少的數量並定期審查檢討。	§13-4 §14-2 §15-1	(1) 針對具有可從外面連線至公司內網之廠商及公司內部人員，建立其帳號權限之申請、異動修改及刪除之管理程序並記錄登入，登出時間。 (2) 將所有的帳號權限列冊管理，並每半年由高階主管及相關人員共同查核檢討一次。 (3) 對其連線紀錄，應每季查核檢討一次，若有異常應立即通報主管處理。
	34	建立存取控制(即帳號權限管理)機制功能，加強對不當資料檔案及存取之檢查。	§15-1 §15-5	(1) 建立帳號權限之申請修改及刪除之管理程序。 (2) 將所有的帳號權限列冊管理，並每半年由高階主管及相關人員共同查核檢討一次。
	35	應確認資訊系統開發設計中已納入必要的安全控管機能。	§15-1 §15-2 §15-4	(1) 資訊系統要開發或修改時，除功能需求外，需針對資訊安全列入要求並落實作業。如密碼一定要 8 碼以上，若未設定為 8 碼，則強制卡關不能到下一步、又如要求網站要在 HTTPS 的通訊加密作業環境等。 (2) 資訊系統/作業系統/通訊軟體等所應用之軟體版本，應強化參數設定及更新至最新版本，即目前使用軟體版本之其弱點已避免或已經有安全處理措施。
設	36	應建立公司資訊設備清冊並定期盤點及檢討資訊設備的	§14-2	(1) 每項設備必須有管理員負責保管，並有設備財產清冊，登記規格資源、服務用途、裝設軟體及 IP。

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
備		安全防護機制。		(2)每年度或半年度執行設備財產盤點作業，並更新設備財產清冊。
	37	識別所有資訊資產之擁有者，並指派維護資訊資產責任。	§14-2	(1)各類設備財產指派人員負責保管。 (2)訂定設備財產之保護要求，例如：筆電、USB 及機敏文件等不用時收到櫃子並上鎖等。 (3)指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。
	38	所有主機及設備在接入網路前，應變更供應商預設之帳號或通行碼，並移除非必要之所有帳號。	§14-2	(1)無論是新購或重新安裝之主機及設備，在正式上線提供服務之前，應檢查相當參數之設定值，並與廠商交接帳號密碼。 (2)與廠商交接帳號密碼後，應立即變更帳號密碼，同時將廠商用的帳號刪除。即每項設備從廠商獲得(交貨安裝後)必須更換帳號密碼。 (3)若帳號無法刪除，則至少應立即變更密碼。
	39	通訊網路及伺服器放置處應有門禁管制；非授權人員進出應填寫進出登記，並由內部人員陪同與監督；進出登記紀錄應定期審查，如有異常應適當處置。	§14-2	(1)儲存個人資料之資訊設備應置放於實體安全區域(如：門禁控管之辦公區域、機房)，避免有心人士或非授權人員存取。 (2)機房作業管理程序及指派負責人員(即需有專人看守)，例如：機房巡查、 進出管制等。 (3)訂定機房進出登記表，以管制人員與設備之進出。 (4)來賓與廠商人員在機房作業時，指派負責人員陪同作業。 (5)外部單位或個人更新或維修電腦設備時，應指派專人在場，確保安全及防止個人資料外洩。 (6)機房進出登記表，主管人員應每週或隨時抽查，若有不符規定或異常應立即採取行動並通知高階主管。
	40	訂定各類設備、應用軟體系	§13-1/§13-2	(1)各類設備財產指派人員負責保管。

類別	項次	建議控制措施	維護計畫 條文對應 (條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		統、儲存媒體之使用、報廢及轉移作業之管理規範。	§14-1/§14-2 §19-4	(2) 訂定各類設備作業使用管理程序，例如：安裝軟體經過誰評估? 誰核准? 誰安裝? 誰維護?作業方式為何? (3) 訂定報廢管理程序，即設備報廢，需有程序將原設備的資訊完整刪除。例如：報廢時要經過誰檢查? 誰核准? 誰刪除或銷毀? (4) 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。 (5) 對使用中之軟體及程式，訂定管制程序，例如：如何修改?如何安裝?誰才可以執行等程序。 (6) 所有紀錄要留存備查。 (7) 防範資料洩漏之建議措施： (a) 有客戶資料之紙張不回收直接銷毀。 (b) CD/硬碟/USB 等不用或故障時，先破壞再報廢丟棄。 (c) 各類設備交接或異動時作檢查，將機密或客戶資料刪除，再交接或異動。