零售業個人資料檔案安全維護管理辦法實務說明

根據《個人資料保護法》第 27 條第 3 項規定，由零售業的中央目的事業主管機關經濟部訂定《零售業個人資料檔案安全維護管理辦法》，適用各類實體店面或兼營網路銷售的零售業者。業者自行或受委託蒐集、處理或利用個人資料檔案，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，以加強管理，確保個人資料之安全維護。

X-FORT 是完整的資料安全防護解決方案，包含 Data Leak Prevention、Data Protection 和 IT Asset Management，防止資訊洩漏遺失，並提供使用者活動記錄與證據保存。

零售業個資防護自評表 X-FORT 對照表

項目	X-FORT 符合
7 資料安全管理	
7.1 是否依據業務作業需要及性質，建立管理機制以規範個人資料蒐集、處理、利用及其他相關流程，並設定所屬人員不同之權限？	行政管理
7.2 是否定期檢視所屬人員不同權限之適當性及必要性？	●
7.3 是否要求所屬人員就所保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他存放媒介物時，應妥善保管個人資料之儲存媒介物？	實體管理
7.4 於傳輸個人資料時，是否依不同傳輸方式（包括但不限於：實體紙本、電子郵件、網際網路、專線），採取適當之安全措施？	●
7.5 有加密必要之個人資料，是否於蒐集、處理或利用時，採取適當之加密措施？	●
7.6 有備份必要之個人資料，是否有採取適當之保護措施？	●
12 設備安全管理措施	
12.1 是否妥善維護紙本資料檔案之安全保護設施及訂定管理程序？	行政管理
12.2 是否將電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制，並訂定管理程序？	●
12.3 是否訂定紙本及電子資料之銷毀程序，並於電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，採取適當防範措施，避免洩漏個人資料？	行政管理
14 使用紀錄、軌跡資料及證據保存	
14.1 是否留存個人資料使用紀錄至少 5 年？	●
14.2 是否留存自動化機器設備之軌跡資料或其他相關之證據資料至少 5 年？	●
15 業務終止後，個人資料處理方法	
15.1 業務終止後，保有之個人資料是否銷毀，並留存銷毀方法、時間、地點及證明銷毀方式等相關紀錄至少 5 年？	行政管理
15.2 業務終止後，保有之個人資料是否移轉，並留存移轉原因、對象、方法、時間、地點，及受移轉對象得保有該項個人資料之合法依據等相關紀錄至少 5 年？	●
15.3 業務終止後，保有之個人資料是否刪除、停止處理或利用，並留存相關方法、時間或地點等相關紀錄至少 5 年？	●

對照零售業個人資料檔案安全維護管理辦法與 X-FORT 控管

以下為 X-FORT 建議使用模組透過對使用者的隨身碟、列印、網路檔案 (雲端硬碟)、通訊軟體 (LINE、WeChat)、電子郵件、軟體使用行為控管及記錄來達到預防資料外洩的目標。

	功能模組	子功能	說明	自評表符合項目
系統管理	用戶端	用戶端管理	• 多重連鎖自我防護，防止惡意移除與破壞 • 監視與記錄使用者活動，備份寫出檔案 • 保護與編碼用戶端記錄；加密上傳用戶端記錄至管理伺服器 • 控管政策可依電腦、使用者、網段設定；依條件自動切換政策，如離線、暫時、RDP • 支援作業系統安全模式下的控管與記錄 • 當用戶端異常時，系統自動發出警示	12.2
本機安控	外接儲存裝置控管	儲存裝置	• 一般外接式儲存裝置防護， 包含外接式硬碟、隨身碟、記憶卡、MP3、播放器等 • 多種控管模式：禁用、唯讀、寫出明文/密文；密文檔案支援連線/離線解密 • 儲存裝置註冊機制：硬體辨識、軟體辨識、序號辨識	7.4 12.2 14.1 14.2
		MTP 裝置	• 多種管理者角色：系統管理員、系統稽核員、群組(部門)管理員及稽核等 • 系統閒置將自動登出用戶端電腦	
		硬碟防護	• 記錄使用者檔案操作行為，包含檔案新增、複製、搬移、刪除等 • 記錄寫出隨身碟、透過網路傳出檔案等行為 • 保留電腦登出登入記錄、WiFi連線記錄、裝置連結電腦記錄	
	進階外接式儲存裝置控管		• 多種明密文寫出模式：群組解密、密碼自解檔、限期自解檔、電腦自解檔 • 線上申請開放控管，寫出檔案需主管審核機制，主管線上審閱內容後核覆 • 限制每日或單一檔案寫出至外接式儲存媒體的檔案大小	7.4 12.2 14.2
	光碟裝置控管		• 可禁用光碟機及燒錄軟體 • X-BURN燒錄：燒錄明文/密文，完整的燒錄記錄及警示；提供主管審核機制，審核後燒錄光碟	7.4 12.2 14.2
	列印裝置控管		• 可控管本機、網路、分享及虛擬印表機，設定不同的列印政策 • 不限應用程式或印表機， 強制列印浮水印 • 列印文件可控管張數、警示，備份列印內容或原始檔案，檔名含特定關鍵字發出警示 • 提供主管審核機制，可申請暫時開放印表機或取消浮水印	7.4 12.2 14.2
	操作記錄	系統檔案	• 記錄系統檔案刪除及檔名異動 (含DOS模式下操作)	7.2 12.2 14.2 15.2 15.3
		使用者日誌	• 記錄軟體執行活動、網頁瀏覽活動 • 記錄用戶端電腦的登入/登出事件 • 記錄檔案操作行為，包含檔案建立、複製、搬移、更名與刪除	
	進階操作記錄		• Microsoft Office 檔案存取記錄： 開檔、存檔、另存的操作記錄 • 剪貼簿文字記錄： 使用者複製、貼上剪貼簿的文字內容	12.2 14.2
	其他控管		• 通訊埠及工具防護：紅外線、藍牙、傳輸線軟體、PrtScr鍵、定位服務、行動裝置同步軟體、遠端遙控軟體、Ghost軟體、VMware軟體、P2P軟體、登錄編輯器、音效卡、無線網卡、USB連接的網卡 • 對電腦裝置清查並鎖定，防止未經許可、未獲授權的裝置連接 • 禁用或允許裝置管理員中的裝置，包含限制裝置類別、PID/VID、列舉程式等 • 提供主管審核機制，允許申請暫時放行指定裝置	12.2

	功能模組	子功能	說明	自評表符合項目
網路安控	共用資料夾控管		• 使用者和外來電腦間的共用資料夾傳輸檔案，可加以禁止、記錄、備份 • 監視共用資料夾的讀取流量、刪檔數目，達到上限時發出警示及e-mail	7.2 7.4 12.2 14.2
	通訊控管		• 內/外通訊埠防護；提供主管審核機制，允許申請暫時開放通訊埠 • 應用程式連線控管：限制應用程式連結網段目的地、通訊埠，防止未經授權連線存取 • 網段流量控管：限制可存取目的網段流量，分別控管上傳量與下載量	12.2
	網頁控管		• 禁止或允許瀏覽HTTP或HTTPS網址 • 符合指定網址時，網頁特殊控管 - 禁止瀏覽器的開啟舊檔、另存、列印、鍵盤、複製、貼上、拖曳出/入網頁 - 記錄與備份上傳檔案 • 網路流量監測：提供每日上傳/下載的資料流量上限警示 • 瀏覽記錄包含搜尋關鍵字、標示連結目的地國家 • 提供主管審核機制，允許申請暫時開放網頁瀏覽	7.2 7.4 12.2 14.2
	Webmail記錄		• 記錄Outlook.com, Gmail, Yahoo! Mail, Openfind Mail2000的Webmail，包含郵件主旨、收件者、內容、附檔名稱 • 備份Yahoo! Mail, Openfind Mail2000附檔	7.4 12.2 14.1 14.2
	雲端控管		• 控管應用程式使用SSL/TLS網路連線，包含雲端硬碟同步軟體 • 依網址關鍵字阻擋連結雲端硬碟 • 複製檔案至雲端同步資料夾即自動加密 • 防止Office另存到雲端硬碟	7.4 12.2 14.2
	傳輸控管		• 通訊軟體 - 禁止執行、禁止傳檔、備份傳送檔案(LINE, WeChat, Tencent QQ, Microsoft Teams, Zoom, Webex Teams, 釘釘, Slack, Chatwork, Telegram, Viber等) - 記錄傳訊內容(LINE, WeChat) • 可禁止或控管FTP/FTPS的上傳/下載行為，含記錄與備份 • 控管無線網路基地台，保留連接記錄	7.4 12.2 14.1 14.2
	電子郵件控管		• 限制可使用的外寄SMTP郵件伺服器寄送郵件 • 記錄及備份使用者寄送的Outlook郵件	7.4 12.2 14.1 14.2
	Outlook附檔加密		• 自動加密：依收件者自動判斷，將Outlook信件的附檔加密後寄出 • 寄送審核：附檔加密的信件先寄給群組管理員，核覆後寄出密碼 • 禁止寄送清單：指定禁止寄送的網域名稱或關鍵字，如任一收件者email符合，自動阻擋該信件 • 防止誤寄郵件：按下傳送時，提示使用者再度確認，防止不慎將郵件寄給錯誤的收件者	7.4 12.2
	SVT伺服器安全通道		• 安裝X-FORT Agent的電腦，才能存取受保護的伺服器 • 指定的使用者或部門，透過身分驗證才能連結受保護的伺服器 • 電腦與受保護伺服器之間的通訊加密，防止網路監聽、竊取機密資料 • 保護對象不限服務類型，支援TCP通訊，不需額外設定或撰寫程式碼	7.2 7.4 12.2

	功能模組	子功能	說明	自評表符合項目
資產管理	軟體安控	應用程式控管	• 清查電腦硬碟內的執行檔，建立白名單 • 比對應用程式屬性，支援應用程式簽章的憑證、檔案雜湊、檔名、路徑，支援父行程關係定義 • 動態白名單管理，支援觀察模式，執行記錄方便快速建立規則	7.2 7.4 7.6 12.2 14.2
		資料夾防護	• 限制特定資料夾中特定副檔名的檔案(如*.exe)，防止未經授權的使用者或程序，在該資料夾中新增、更名特定副檔名的檔案 • 限制用戶端電腦中特定資料夾內的檔案，只能被指定的信任程式存取，確保資料夾內的資料，不被其他非授權程式存取，或加入檔案	
		軟體執行控管	• 記錄禁止或非允許的軟體執行；依時段管理禁止或允許執行軟體 • 提供主管審核機制，允許申請暫時開放使用軟體	
		安全備份	• 定時自動備份資料夾，並限制應用程式存取備份目的，確保備份安全 • 搭配資料夾防護，確保備份目錄不被破壞	
			• 軟體執行時，管制特定功能，禁止開啟舊檔、另存、列印、鍵盤、複製、貼上、拖曳出/入程式、上傳檔案 • 軟體執行時，記錄與備份以滑鼠拖曳入或開啟舊檔方式產生的上傳檔案行為 • 軟體執行時或常態啟動螢幕浮水印，浮水印文字支援漸層與透明度，不易被背景色屏蔽	
遠端管理	畫面擷取		• 單一畫面擷取，如視窗切換、使用剪貼簿、Microsoft Office另存新檔 • 固定時間間隔連續擷取，如執行特定軟體、網頁清單 • 可自訂影像品質、解析度、顏色及間隔時間條件 • 矩陣瀏覽(GridView)畫面記錄；匯出單張畫面圖檔，或連續畫面影片檔	14.2
EDR事件反應	行為偵測與反應		• 監視及偵測違規行為，主動反應控制風險 • 用戶端自動反應包含螢幕浮水印、警示、限制網路傳輸、禁用隨身碟、禁用印表機等；管理者可遠端執行命令(如強制關機、遠端命令等)、復原用戶端發生之自動反應 • 自適應政策：透過EDR組合偵測執行特定程式、電腦所在位置、RDP遠端連線等組合為偵測條件，條件觸發自動切換控管政策 • 記錄各種違規事件、反應動作與處置方式	12.2 14.2

資料保護	內容過濾與分類		• 內建範本支援正規表示式(RegEx)、關鍵字過濾
			• 過濾中文姓名、地址、電話等個資(需額外選配)
			• 本機出口管制
			  - 外接儲存媒體寫出檔案、通訊軟體傳送檔案、Outlook寄送本文及附件，依過濾比對結果阻擋或放行；放行時可備份檔案，並加註過濾摘要至記錄
			• Webmail過濾
			  - 寄送Webmail (Yahoo! Mail, Openfind Mail2000) 後，過濾比對郵件本文和備份附件，加註過濾摘要至記錄
			  - 寄送Webmail (Gmail, Outlook.com) 後，過濾比對郵件本文，加註過濾摘要至記錄
			• ※需搭配購買控管模組 (如：外接式儲存裝置控管、傳輸控管、電子郵件控管、網頁控管、Webmail記錄等)
				7.4
				12.2
				14.1
				14.2

	File Locker		• 使用者可自行決定檔案加密保護，支援單一或批次檔案加密 • 不改變使用者操作習慣，雙擊加密檔自動解密，檔案關閉自動加密 • 清查用戶端檔案副檔名，並強制加密 • 中央控管設定加/解密政策，對用戶端檔案及資料夾強制加密 • 管理者可限制開啟解密的人員、離線解密可使用天數 • 使用者可設定檔案加密資料夾，自動監控資料夾新增檔案立即自動加密；支援根目錄、雲端同步目錄(不支援Server OS) • 搭配內容過濾與本機安控出口控管功能，達到阻擋或保留寫出記錄	7.4 7.5 12.2 14.2