電商安維辦法實務說明

依據個資法第 27 條規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取。數位發展部為數位經濟相關產業之中央目的事業主管機關，為使相關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，並提供電腦資產盤點、應用程式管理及遠端遙控的管理系統。

數位發展部所管電商業者個資防護企業自評表 X-FORT 符合表

項目	X-FORT 符合
1. 人員及資源配置（安維辦法第 3、4、5 條）	
1.1 已配置專責人員或組織管理及維護保有之個人資料。	
1.2 已配置適當資源 (如軟硬體設施及經費等) 執行個人資料保護相關事項。	●
1.3 已訂定及配合相關法令修正個人資料保護管理政策。	
1.4 已訂定及配合相關法令修正個人資料檔案安全維護計畫。	
6. 資料安全與人員管理（安維辦法第 11、12 條）	
6.1 是否進行去識別化作業？	
6.2 是否有資料存取控制措施？	●
6.3 是否進行檔案加密？	●
6.4 是否進行資料備份，並對備份資料採取適當之保護措施？	●
6.5 資料之傳送是否進行管控？	●
6.6 使用資訊系統或其他系統進行個人資料交換時，是否有採取適當保護措施？	●
6.7 是否建置防火牆、電子郵件過濾機制或其他入侵偵測設備，並定期更新及執行惡意程式檢測。	
6.8 是否有遠端存取控管措施？	●
6.9 電腦、相關設備或系統有定期檢測並因應系統漏洞所造成之威脅。	
6.10 保有資料者是否遵守保密協定？	
6.11 人員進出情形是否具體掌控？	
10. 紀錄保存（安維辦法第 16 條）	
10.1 是否保存個資（含紙本及數位檔案）管理紀錄（如存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄？）	●
10.2 管理含有個人資料之資訊系統，是否已建立必要之使用紀錄、軌跡資料（Log Files）及證據之保存措施？	●

* 安維辦法：全名為「數位經濟相關產業個人資料檔案安全維護管理辦法」

對照安維辦法與 X-FORT 控管

以下模組為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	1.2
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	6.2 6.3 6.4 6.5 6.6 10.1 10.2
		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	
	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		6.2 6.5 10.1 10.2
	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)	10.1 10.2
		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		

網路安控	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
				6.2
				6.5
				10.1
				10.2

	傳輸控管	• 即時通訊軟體可禁止執行、禁止傳檔、禁用截圖、禁用桌面分享；記錄傳訊內容、備份傳送檔案&截圖內容 (LINE, Skype, Tencent QQ, WeChat, 阿里旺旺) • 視訊會議軟體可禁止執行、禁止傳檔；備份傳送檔案 (Microsoft Teams, WhatsApp, Zoom, Webex Meetings, Webex,Teams, 釘釘, BlueJeans, GoToMeeting, Slack, Chatwork, Telegram, Viber) • 可禁止或控管FTP/FTPS的上傳/下載行為， 含記錄與備份 • 禁用3G/4G網卡撥接軟體、分享網路（行動熱點） • 控管無線網路基地台，保留連接記錄		6.2 6.5 10.1 10.2
	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		6.5

	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	6.8
		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	• 記錄使用者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	6.4
		• 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		6.8
資料保護	內容過濾與分類	• 內建正規表示式(RegEx)、關鍵字過濾 • 本機出口管制 - 過濾檔案內容，依比對規則阻擋、放行，備份之附加檔案，加註標籤至記錄，包含寫出外接儲存媒體、通訊軟體傳檔、電子郵件Outlook附檔 • Webmail過濾 - 寄送Webmail (Yahoo! Mail, Openfind Mail2000) 後，過濾比對郵件本文與附件，備份附件檔案副本，並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		6.2 6.5 6.6 10.1 10.2