網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
策略面					
1.依據公司資安政策，落實資安管理					
1.1 是否制定適用之資訊安全政策並公告周知(含員工、委外廠商、上下游合作廠商)？					
1.2 是否訂有涵蓋電子商務核心營運系統資訊安全作業之內部稽核計畫(含稽核目標、範圍、時間、程序、人員)，並定期辦理內部稽核？					
1.3 內部稽核後是否產生稽核報告並追踪改善情形(包括稽核發現的摘要、稽核區域、缺失說明及改進建議等)？					
1.4 是否指定專人或專責單位，負責辦理資安政策、計畫、措施之研議，資料、資訊系統之使用管理及保護，資安認知、教育、訓練、資安稽核等資訊安全範圍內之工作事項？					
1.5 管理階層是否有要求員工、產業供應鏈上下游業者及第三方使用者，依照公司已制定的政策與程序施行安全事宜？					
2.資安教育訓練與宣導狀況					
2.1 管理階層是否有要求員工、產業供應鏈上下游業者及第三方使用者，依照公司已制定的政策與程序施行安全事宜？					
2.2 是否對所有員工、產業供應鏈上下游業者及第三方使用者提供妥適等級之有關安全程序及資訊處理設施的正確使用之認知教育與訓練？					
2.3 員工離職或第三方使用者於聘雇終止時，是否依規定繳回其使用或保管之資訊資					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
產？(包含歸還所有先前發出的軟體、公司文件、設備、行動裝置、存取卡、軟體、手冊及儲存於電子媒體的資訊等公司資產)					
2.4 是否於所有員工、產業供應鏈上下游業者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、契約或協議終止時，或因變更而調整時，予以移除？					
2.5 是否確保公司內任何人從事電子商務服務時，應注意並保持充分了解維護客戶隱私？					
2.6 是否定期評估需進行主機或相關軟體漏洞之更新？如需更新，則於不影響運作前提下進行更新。					
管理面					
3.風險評鑑、資訊資產清查與管理					
3.1 是否鑑別所有資產可能遭遇之威脅？					
3.2 是否鑑別所有資產可能之脆弱點？					
3.3 是否鑑別資產可能因威脅發生而喪失機密性、完整性與可用性之衝擊？					
3.4 是否制定風險處理計畫並根據該計畫導入控制措施以降低風險？					
3.5 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有妥適分工與分散權責？					
3.6 被賦予敏感資訊存取權的所有員工、產業供應鏈上下游業者及第三方使用者，是否					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？					
4.個人資料保護與管理					
4.1是否有個資管理人員組織配置？並依分工執行？					
4.2是否有個人資料保護管理政策？是否公告公司人員周知？					
4.3就個資之蒐集、處理、利用是否有相關程序規定？是否公告公司人員周知？					
4.4是否進行個資盤點並備有清冊？盤點之方式為何？結果之正確性？					
4.5是否進行風險分析並進行相應處理？風險分析之方式？結果之正確性？					
4.6針對事故是否有可行之應變機制？					
4.7蒐集處理利用是否具備並符合特定目的及特定情形？是否遵守其他依法令應遵守之事項？					
4.8是否有特定目的外利用？如有，是否有合法事由？					
4.9是否進行行銷？行銷是否符合特定目的？如進行行銷是否提供當事人拒絕行銷之管道？是否於當事人拒絕行銷時，停止行銷？					
4.10特定目的消失或期限屆至時，是否刪除、銷毀、停止蒐集、處理、利用個資？如否，有無法定事由？					
4.11業務終止時是否對個資進行妥善、合法之安排？					
4.12是否進行告知？如否，有無					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
法定免告知事由？告知之時點與方式是否合法、適當?					
4.13有無蒐集、處理、利用特種資料？如有，其蒐集、處理、利用及其他相關規定是否已遵守？					
4.14是否主動更正或補充當事人之個人資料？					
4.15是否提供當事人權利行使管道？是否於法定期限內回覆當事人？如展延回覆時期，是否依法定要式為之？拒絕當事人時是否有合法事由？					
4.16是否曾（合法）提供資料予第三人？如提供內容有誤或不備之資料如何通知更正？					
4.17發生個資事故時是否適時通知當事人？					
4.18針對個資檔案特性、流程及所處環境，其物理面、技術面、作業及系統面之安全管理措施為何？是否符合功能角色取向、最小化、風險管控決策之要求？後續如何持續改善以處理剩餘風險？					
4.19如何決定是否委外？委外時如何選任受託人？與受託人間是否就個資法所要求各各事項簽訂合約或設計監督規劃？					
4.20是否對人員進行必要教育訓練？					
4.21發現不足時是否加以矯正或預防？					
4.22是否自行進行稽核或委外稽核？委外稽核時，當稽核之內部人員或外部稽核人員是否有足夠之法律及稽核能					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
力？					
4.23是否定期檢視個資管理之狀況並持續改善？					
5.委外服務作業之資訊安全					
5.1 是否針對服務供應商之信譽考量進行以下之評估項目？ (1) 具有一定之知名度且在業界商譽良好。 (2) 相關金融徵信紀錄良好。 (3) 具有知名企業客戶，經徵詢後無不良品質紀錄。 (4) 無重大資訊安全事件之紀錄。					
5.2 委外廠商需使用電子商務營運相關平台或進入相關營業單位工作時，其所申請門禁進出權限或資訊系統與網路資源之使用帳號，是否依資訊安全相關單位之管理程序辦理？					
5.3 是否根據雙方的正式契約，擬定委外廠商對電子商務營運平台資訊處理設備的存取權限，內容並包含或提及所有的安全要求？					
5.4 委外廠商是否未擁有營運系統及客戶資料之控制權？且需保護和控管相關客戶資料之安全。					
5.5 委外物流服務業者，其資訊安全管理要求應包含商品進倉、撿貨、配送資料整理、定點集中運送(包含店取及超取)、到府宅配、退換貨等逆物流服務流程。					
技術面					
6.核心營運系統取得、開發及維護安全管理					
6.1建置核心營運系統是否備有					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
系統分析與設計文件？					
6.2核心營運系統在規劃需求時是否將相關安全要求納入分析及規格？					
6.3處理客戶個人資料檔案資訊系統之開發，是否避免以真實個人資料進行測試？如需使用，是否於完成測試作業後立即移除，或將可辨識之個人資料修改為無法辨識之模糊資訊？					
6.4核心營運系統程式碼存取與更新作業是否限定授權人員或負責人員才可執行？					
6.5是否建立新系統或系統升級及新版本之驗收準則，並只有在正式驗收後，新資訊系統、系統升級及新版本才可移轉上線(含驗收標準及應有之測試)？					
6.6是否設定適當的使用者註冊與取消註冊規定，以對所有核心營運系統核准和取消其存取權限？					
6.7核心營運之系統使用者因變更權責、調職或離職後，是否立即移除、封鎖或變更其存取權限？					
6.8是否避免讓輸入之使用者通行碼以明文方式顯示在螢幕上？					
6.9是否針對核心營運系統登入之通行碼輸入錯誤或登入失敗，訂有一定次數以下之限制(如：登入失敗三次以上即將帳戶予以鎖定或強制延遲一段時間)？					
6.10 敏感之紙本、USB 隨身碟、					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
隨身硬碟，是否未置於不受保護之桌面上？					
6.11 主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時，是否採用保護措施？					
6.12 是否依據核心營運系統之網路服務需要，區隔出獨立的邏輯網域(如：公司內部網路、核心營運系統網路、DMZ 區、外部網路等)？					
6.13 各獨立邏輯網域是否皆有建置如網路防火牆之通訊閘道，管制過濾網域間資料的存取？					
6.14 執行敏感性資訊處理(如：客戶資料)之電腦是否不允許上網或進行網路隔離？					
6.15 是否不允許使用者使用不必要之系統公用程式(如：遠端連線、telnet)？					
6.16 核心營運系統是否具有作業結束後、或在一定期間未操作時即自動登出之保護機制？					
6.17 設備汰除前是否將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？					
6.18 對外交易平台是否經由防火牆連接後端資料庫？或確認於內部網路區域(如：從 DMZ 隔離開來的)中使用資料庫。					
6.19 內部任何允許連接客戶資料庫的電腦，是否一律不允許直接連上網際網路，並限制周邊存取(USB)行為？					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
6.20 針對資料庫系統已知漏洞，若在不影響現行作業狀況下，是否立即進行修補？					
6.21 資料庫管理者之操作行為是否記錄？					
6.22 資料庫系統應啟動記錄功能，是否至少但不限於保存以下紀錄？(1) 使用者帳號新增、刪除等異動紀錄。(2) 特殊權限之異動紀錄。(3) 稽核功能的啟動、停止紀錄。(4) Object 之 Drop、Delete 紀錄。(5) Table 之 Create、Drop。(6) 稽核資料的修改、刪除紀錄。					
7.對外網站交易安全管理					
7.1是否定時評估網站伺服器上線流量，以維持系統效能需求？					
7.2是否使用網路安全防禦設備，並適當的隔離外部網際網路與公司內部網路？					
7.3是否針對機敏資料的安全需求，進行資料加密與控管機制的評估與落實，並留存使用紀錄？					
7.4是否建有帳戶登入預防(如程式無法解讀之英數字)與鎖定機制，以阻止惡意暴力密碼破解攻擊？					
7.5是否禁止共用帳戶和密碼？					
7.6 是否要求使用者使用強度較高的密碼，並建立控管機制？					
7.7 是否制定適當之控制措施，以保護含有資訊的文件或儲存媒體在公司範圍外傳送時，不受未經授權的存取、誤					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
用或毀損？					
7.8 高度機敏性的資訊，在內部或供應鏈上下游傳輸或儲存時，是否使用加密技術(如：VPN, SSL, HTTPS 等)？					
7.9 當通過公共網路傳輸敏感的持卡人資料時，是否使用 SSL 或其他行業可接受的方法進行加密？					
7.10 交易帳戶資訊是否儲存於位於內部網路(非 DMZ)的資料庫，並用防火牆加以保護？					
7.11 交易頁面是否提供安全的傳輸通道給使用者傳輸機敏資訊(如：輸入密碼或信用卡號時)？					
7.12 是否定期檢查防火牆、路由器、無線接入點和驗證伺服器的日誌，以防範未經授權的交易發生？					
7.13 所有對外開放的網頁應用程式和系統在上線前是否進行弱點掃描和滲透測試，並進行修補作業？					
8.網路通訊與資訊作業安全管理					
8.1 是否全面使用合法防毒軟體，並即時更新病毒掃描引擎及病毒碼？					
8.2 是否界定處理電腦病毒、木馬等惡意程式的作業要點與責任，訓練員工通報惡意程式之攻擊，並執行復原程序？					
8.3 資料庫備份資料之存放地點是否進行控管，防止非相關人員存取？					
8.4 是否定期檢測網路運作環境之安全漏洞？					
8.5 電子商務作業之電子郵件伺					

網路零售業者個資防護廠商自評表

日期：104 年　月　日

★主管機關行政檢查將依據本【網路零售業者個資防護廠商自評表】及【現場查檢】作整體資安綜合評估，請廠商確實填寫。

查檢項目	自評內容				簡述原因
	符合	部分符合	不符合	不適用	
服器管理，是否考量參考「電子商務郵件安全機制控制項」，執行相關控管作為？					
8.6是否使用適當之網路安全解決方案(如防火牆、入侵偵測系統)？防火牆存取政策(security policy)設定是否適當？					
8.7各項日誌是否有適當的保護措施，不受竄改與未經授權的存取，並針對留存之通信資料設定適當之留存期限？					
8.8是否留有詳細的管理者與操作員所涉及的過程之作業日誌，系統管理者與操作者日誌是否定期予以審查？					
8.9是否注意不隨意開啟郵件附件與郵件內容中不明之超連結？					
8.10使用者是否了解電子郵件社交工程威脅？					
8.11是否訂定電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)之控制措施？					
8.12執行電子商務作業之電子郵件信箱之使用者登入密碼，是否設定至少 6 碼以上？					
8.13電腦內之作業系統，是否符合公告之標準，並安裝最新的修正程式？					
8.14執行電子商務營運之個人電腦(含筆記型電腦)作業系統與電子商務相關應用程式之使用者登入密碼，是否設定至少 6 碼以上？					