101 年度電子商務交易安全及資安服務平台推動計畫

電子商務交易安全規範
(網路平台、供應商、物流商)修正版

財團法人資訊工業策進會編製

中華民國 101 年 11 月

內容摘要

為提升電子商務供應鏈之電子商務平台業者之資訊安全管理、商品供應商(或賣家)的資訊管理與物流商資訊管理流程等之作業安全需求，特召集產業代表、專家學者、顧問單位共同參與規劃、審查並修正「電子商務交易安全規範」(下稱本規範)，做為我國電子商務產業相關業者之行政參考文件，本規範依實施對象分別編纂 3 份規範文件：

一、 電子商務交易安全規範-網路平台 1 式

二、 電子商務交易安全規範-供應商 1 式

三、 電子商務交易安全規範-物流商 1 式

以有助於電子商務業者致力提升交易安全、強化消費者安全信賴時，於各項管理面、作業面之實務參考。

成果對應文件

成果名稱	對應文件
電子商務交易安全規範(網路平台、供應商、物流商)修正版	電子商務交易安全規範 V3.0 版-網路平台
	電子商務交易安全規範 V3.0 版-供應商
	電子商務交易安全規範 V3.0 版-物流商

網路平台交易安全規範

經濟部商業司

電子商務交易安全規範
網路平台

規範、進階指引及查檢表

V3.0 版

指導單位：經濟部商業司
主辦單位：財團法人資訊工業策進會
執行單位：中華無店面商務發展協會
中 華 民 國 １０１ 年 １０ 月

目錄

圖目錄

表目錄

壹、前言

一、依據

經濟部商業司(下稱商業司)「101 年度電子商務交易安全及資安服務平台推動計畫」(下稱本計畫)。

二、主旨

為提升電子商務供應鏈之電子商務平台業者之資訊安全管理、商品供應商(或賣家)的資訊管理與物流商資訊管理流程等之作業安全需求，特召集產業代表、專家學者、顧問單位共同參與規劃、審查並修正「電子商務交易安全規範」(下稱本規範)，做為我國電子商務產業相關業者之行政參考文件，本規範依實施對象分別編纂 3 份規範文件：

(一) 電子商務交易安全規範-網路平台 1 式

(二) 電子商務交易安全規範-供應商 1 式

(三) 電子商務交易安全規範-物流商 1 式

以有助於電子商務業者致力提升交易安全、強化消費者安全信賴時，於各項管理面、作業面之實務參考。

三、電子商務定義

我國行政院主計總處所編印之「中華民國行業標準分類」，其主要目的在於提供統計分類之用，行業標準分類原則主要係參酌聯合國國際行業標準分類(International Standard Industrial Classification of All Economic Activities, ISIC)中以場所單位之主要經濟活動作為分類基礎之架構。其中關於電子商務之定義，依據聯合國國際行業標準分類第 4 次修訂版(ISIC Rev.4)之定義為:「企業單位接到訂單後，以各種電子媒介方式處理所生產之商品及服務之交易，例如藉由電話、傳真、電視、電子資料交換(EDI)及網際網路。」亦即所有從事

商品或服務之所有權移轉，是藉由網際網路或其他的電子媒介所為的商業交易行為就稱之為電子商務。

另依據商業司在「2011 電子商務年鑑」，將電子商務定義為：「運用先進資訊科技，同時藉由組織作業的流程改造，來達到減低組織營運的成本開支，提升作業效率，增加客戶滿意度之商業活動。」亦即利用電腦或新興手持式電子產品，例如智慧型手機、平版電腦等，透過網路進行買賣交易之行為皆稱之為「電子商務」。如商業 EDI(Electronic Data Interchange)、金融 EDI、網路銀行、網路購物等行為，都涵蓋在電子商務範疇之中。

四、目的

本規範文件之制定，除參考我國資通安全管理相關規範、CNS 27001:2005 資訊安全管理標準、個人資料保護法及其他國際標準中與電子商務產業相關的規範，據以規劃本規範文件之框架，並依據以下目的，訂定適合企業交易安全實務操作之文件。

(一) 依電子商務業者之營業額、個資量、作業特性等分級分類，不同等級給予不同的資安防護實施建議。

(二) 3 份交易安全規範，至少涵蓋以下作業流程，以利電子商務業者掌握上下游作業之資訊安全。

1. 電子商務供應鏈之中大型電子商務平台業者之資訊安全管理。
2. 含內部資訊流管理。
3. 交易網站安全機制管理。
4. 有效的交易網站安全機制。
5. 與供應鏈的協同資訊作業管理。

6. 商品供應商(或賣家)的資訊管理(含交易資訊管理流程)。

7. 物流商資訊管理流程(含客戶資料保護管理)。

8. 作業安全需包含交易資訊之機密性、交易平台之可用性、交易內容之完整性、與交易作業之適法性等需求。

貳、文件說明

一、適用範圍

(一)「電子商務交易安全規範-網路平台」適用對象為電子商務平台業者，其類型包含如下，並不加以第一類、第二類區分，規範要求皆適用。

1. B2C 平台商：使用電子商務技術，直接提供消費者商品購買服務之廠商。

2. B2B2C 平台商：提供網路交易平台，由個別網路商家參與，使用電子商務技術，直接或間接提供消費者購買服務之廠商。

(二)「電子商務交易安全規範-供應商」適用對象為配合網路平台電子商務交易，提供直接或間接 B2C 商品經銷或銷售之代理業者、經銷業者、零售業者或電子商家。不涉入 B2C 商品交易之訂購服務、客服服務、金流作業、配送服務等流程之商品製造、輸入、代理、經銷或銷售等業者，不包含在本規範之適用範圍中。

1. 第一類供應商為：只有擁有一般網際網路連線、使用一般網站(Web)交易系統及一般辦公室使用之 OA 電腦設備之供應商。

2. 第二類供應商為：擁有或租賃或委外之網際網路專線、營運系統或其他與電子商務相關應用系統之供應商，或與網路平台、物流商之間，透過後台連線交換傳遞或拋轉客戶之會員資料、訂購資料、交易金額、配送資料之供應商。

(三)「電子商務交易安全規範-物流商」適用對象為配合網路平台電子商務交易，提供直送或轉運 B2C 境內(含離島)商品配送服務

流程之汽機車快遞業者、路線貨運業者、宅配業者、郵遞業者，以及提供取貨服務之實體商店等。跨境之海陸空運承攬業者、倉儲流通轉運業者、大型批發物流流通業者等不涉入 B2C 商品配送服務的作業流程，不包含在本規範適用範圍。

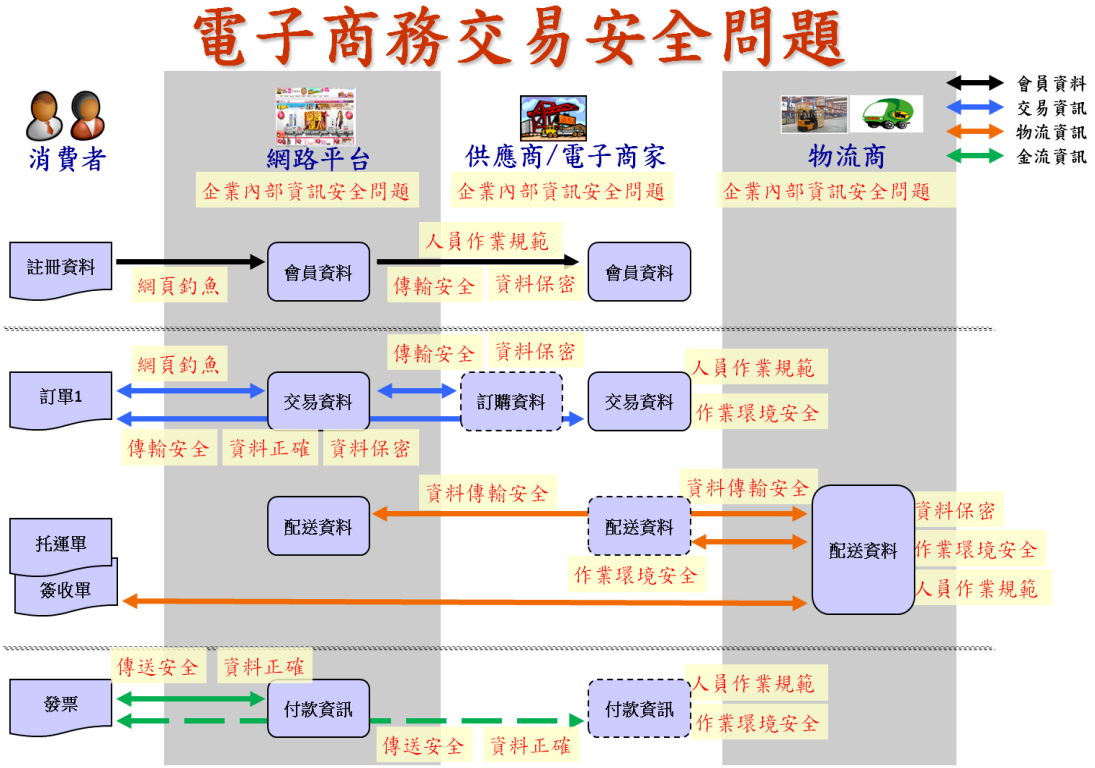
1. 第一類物流商：僅接觸紙本(含印出之配送單、簽收單及手寫快遞單正副本)配送資料之物流商。
2. 第二類物流商：與網路平台、供應商之間，有連線或離線的電子資料交換、傳送等作業流程之物流商，或其本身擁有物流服務網路平台、物流配送作業管理系統等之物流商。

二、規範之文件位階

本規範主要為電子商務產業專用之二階規範暨三階指引。二階規範定義為電子商務業者依據分級所必要遵循或執行之安全作為；規範內容多數係依據相關法令法規與國際標準要求制定。三階指引將提供電子商務業者為強化交易安全與客戶資料保護之進階資安作為參考；規範內容係依據國內外各項資安實作手冊制定，並參考連結至商業司相關資安規範。

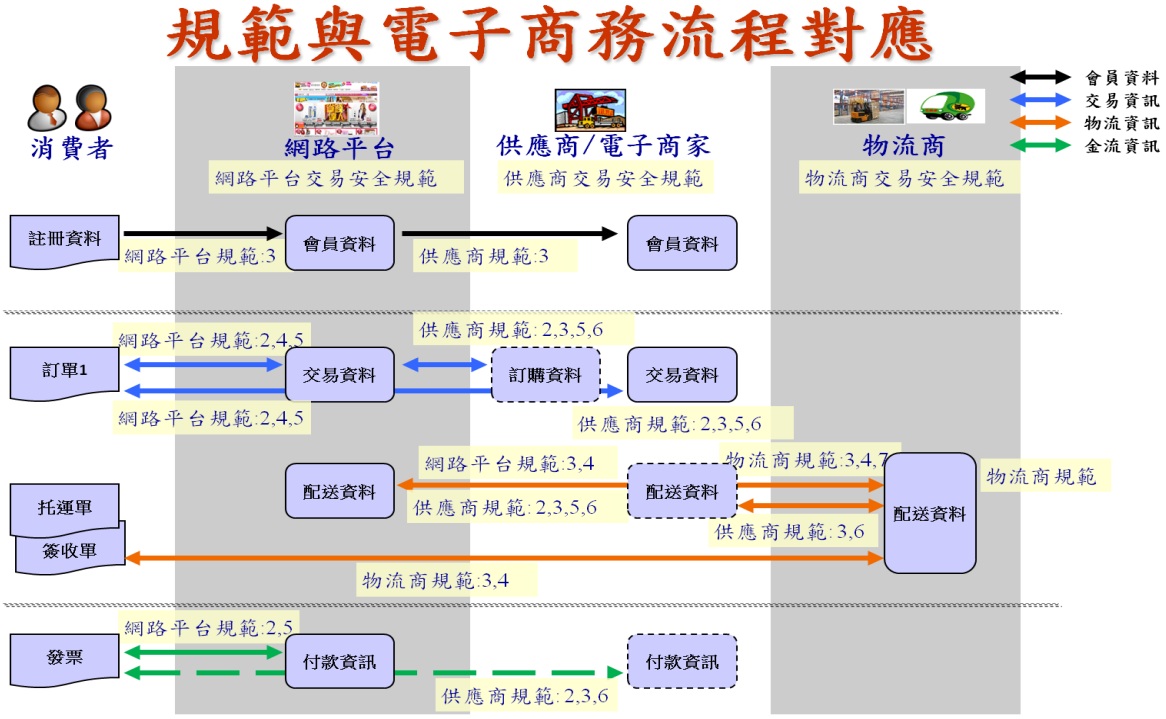
三、電子商務交易安全規範與實施策略目標

依據規範適用範圍之電子商務業者，所涵蓋之交易服務上下游作業流程，為確保實施 3 份規範能達成之交易安全提升，爰依據上下游作業流程中，應予以保護之重要資訊流(如圖 1、2，表 1)，訂定相對應之實施策略目標。



資料來源：本計畫整理

圖 1　交易服務上下游作業流程重要資訊流與安全問題



資料來源：本計畫整理

圖 2　交易服務上下游作業流程與規範實施策略目標對照

表 1　電子商務交易安全規範實施策略目標

文件名稱	電子商務交易安全規範-網路平台	電子商務交易安全規範-物流商	電子商務交易安全規範-供應商
實施策略目標	1.促進組織資訊安全管理	1.促進組織資訊安全管理	1.促進組織資訊安全管理
	2.加強核心營運系統與資料庫之安全管理	2.加強核心資訊系統安全管理	2.建立營業資訊設備管理
	3.強化客戶個人資料安全管理	3.保護客戶個人資料檔案安全	3.保護客戶個資及作業資料安全
	4.提升企業內資訊環境安全管理	4.建立託運單安全管理	
		5.加強作業環境安全管理	4.加強作業環境安全管理
		6.加強網路安全管理	5.加強網路安全管理
	5.強化對外網站交易平台安全管理	7.建立外部單位資料交換安全管理	6.建立外部單位資料交換安全管理
	6.建立資安通報管理機制	8.建立資安通報管理機制	7.建立資安通報管理機制

資料來源：本計畫整理

四、資訊安全框架

因 ISO 27001/ISO 27002 之資安管理領域架構，為國內與國際最多機構(含電子商務產業)之產業資安標準之參考框架，因此將之列為本規範框架之主要依據。

為補足 ISO 27002 之實作指引對個資管理的深度不足，本規範將另行依據最新之個資法所規範之管理精神，強化電子商務產業客戶個資管理。

五、規範文件結構

(一) 文件結構

為依循電子商務產業特性，以制定管理面、作業面的可達成之原則性的交易安全規範。故將規範文件分為策略目標、規範大綱、要求項目與進階指引共四層之文件結構。

(二) 規範共分為四層

第一層為提升電子商務交易安全之策略目標；

第二層為達成個策略目標之管理項目；

第三層為各管理項目下之具體要求項目；

第四層為達成要求項目之必要或參考查檢表；

查檢表之檢核紀錄欄位亦列出於交易安全執行現況中，可作為佐證資訊之相關建議，以提供業者實施本規範之操作面參考。

表 2　規範內容示例

管理項目	要求項目	類別	依據之法規或標準
策略目標：1.促進組織資訊安全管理			
1.1　資訊安全框架	1.1.1 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。	皆適用	ISO 27001
	1.1.2 電子商務網路平台管理階層，應具體說明其對資安之承諾與責任。	皆適用	ISO 27001

資料來源：本計畫整理

(三) 查檢表

1. 為有利於網路平台業者依營運現況進行分類分級實施，並使企業自我檢查或外部第三方查核能有所依據，爰依照各要求項目制定查檢表。除前述之基本遵守的規範要求以外，特於

查檢表中訂定進階指引操作項目，以提供企業參考使用。

2. 查檢表中標示“II”表示僅第二類業者適用。

3. 針對各項規範要求，本規範提供業者必要執行之作業基準查檢項目，及進階查檢項目(進階指引欄位標示◎)。

4. 作業基準查檢項目(Baseline，簡稱 BL)，係為達成各要求項目之交易安全風險基礎管理工作，業者必要且至少應執行之控管作為。

5. 進階查檢項目(Better Practice，簡稱 BP)，係依據各項國際資安實務準則，提供業者參考之進階控管作為，業者得依據資源與風險現況自行決定是否執行。

表 3　查檢表內容示例

編號	要求之查檢項目	類別	進階指引	檢核結果	檢核紀錄
1. 促進組織資訊安全管理					
1.1 資訊安全框架					
1.1.1 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。					
1.1.1.1	是否制定全公司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)？	皆適用		□ 符合 □ 不符合	□ 制定政策，內容包含： - 資訊安全的目標 - 概要資訊安全原則的需求 - 公司內部權責 □ 政策公告內部員工 □ 政策公告給外部廠商 □ 政策定期審查與更新

資料來源：本計畫整理

(四) 附錄

為利於業者對照 ISO 27001、ISO 27002、個人資料保護法以及規範中參考引用之其他管理標準，將規範依查檢項目編號與其對應之法規或標準以及其他可供規範時做參考來源，編列參考文件索引表於附錄中。

另將 3 份規範常見名詞，增列其名詞釋義表於附錄中，但未以所有相關標準出現名詞為涵蓋範圍。

六、未盡事宜

本規範制定時依產業現況與需求，考量文件位階、制定目標、適用範圍及業者實施可能遭遇困難及資源限制，以及目前相關法令法規、產業標準版本發布內容等因素，其有未盡事宜，非為規範之執行限制。已導入相關資訊安全標準之業者，仍建議以符合企業經營及競爭力提升之需求，充分涵括電子商務交易安全相關作業流程或企業整體資訊安全管理流程，施予應有及必要之安全保護，以利電子商務信賴安全環境之發展。

參、規範概述

一、整體大綱

本(網路平台)交易安全規範 6 大實施策略目標下，共計 28 個管理項目，93 條要求規範，皆為應執行之作業基準(Baselines)。規範之下共提供 479 條查檢項目供業者查檢之參考，其中 211 條查檢項目為進階指引(Better Practices)，可依據風險管理需求選擇性執行，或依實際執行情形紀錄查檢結果。

二、規範導入及 ISO 27001 符合性說明

本(網路平台)交易安全規範 6 大實施策略目標與 ISO 27001 管理領域之對照如下，通過 ISO 27001 驗證之業者，可依其資訊安全管理制度適用性聲明文件中，已適用之管理領域與控制項目，對照規範管理項目，以有助於確認規範符合性或強化既有資訊安全管理制度之參考。

表 4　網路平台交易安全規範實施範圍

策略目標	管理項目	實施範圍	規範項目數
1.促進組織資訊安全管理	1.1 資訊安全框架 1.2 風險管理 1.3 資訊資產管理 1.4 人力安全管理 1.5 遵循性管理 1.6 委外管理	- 管理階層 - 人力資源管理部門(包含委外廠商) - 法律遵循性管理部門(包含智慧財產權、個人資料保護法、消費者保護法等) - 資產風險管理部門	15
2.加強核心營運系統與資料庫之安全管理	2.1 核心營運系統取得、開發及維護安全管理 2.2 核心營運系統存取控制管理 2.3 核心營運系統機房與作業環境實體安全	- 負責電子商務交易平台或重要核心營運系統維運管理部門 - 負責系統開發、系統存取控制、機房	21

策略目標	管理項目	實施範圍	規範項目數
	2.4 核心營運系統資料庫安全管理 2.5 核心營運系統營運持續安全管理	與作業環境、營運持續等作業流程之執行單位	
3.強化客戶個人資料安全管理	3.1 客戶資料隱私管理 3.2 客戶資料盤點作業 3.3 客戶資料依法對外公開、資訊揭露作業 3.4 客戶資料蒐集、處理及儲存管理作業 3.5 客戶資料使用及傳輸安全作業 3.6 客戶資料正確性維護作業 3.7 客戶資料刪除及停止利用作業	- 涉及客戶個人資料之作業部門與其作業流程	23
4.提升企業內資訊環境安全管理	4.1 網路通訊與資訊作業安全管理 4.2 電子郵件安全管理 4.3 個人資訊設備安全管理 4.4 網際網路內容瀏覽管理	- 負責公司整體網路通訊、資訊作業環境管理之執行單位 - 所有使用企業與電子商務相關業務之使用者	15
5.強化對外網站交易平台安全管理	5.1 客戶隱私保護政策宣告作業 5.2 交易網站伺服器與網路環境安全管理 5.3 線上交易安全管理 5.4 交易網站技術弱點管理	- 負責對外營業交易網站維運管理部門及執行單位	15
6.建立資安通報管理機制	6.1 電子商務資安通報機制 6.2 資安事故管理	- 管理階層 - 負責資訊安全事故管理執行單位	4
小計			93

資料來源：本計畫整理

表 5　網路平台交易安全規範與 ISO 27001 符合性對照

策略目標	管理項目	ISO 27001 管理領域對照
1.促進組織資訊安全管理	1.1 資訊安全框架 1.2 風險管理 1.3 資訊資產管理 1.4 人力安全管理 1.5 遵循性管理 1.6 委外管理	- 本文(4.2, 4.3,6) - 組織管理(A.6) - 資產管理(A.7) - 人員安全管理(A.8) - 通訊與作業管理(A.10) - 存取控制管理(A.11) - 遵循性管理(A.15)
2.加強核心營運系統與資料庫之安全管理	2.1 核心營運系統取得、開發及維護安全管理 2.2 核心營運系統存取控制管理 2.3 核心營運系統機房與作業環境實體安全 2.4 核心營運系統資料庫安全管理 2.5 核心營運系統營運持續安全管理	- 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 資訊安全事故管理(A.13) - 營運持續管理(A.14) - 遵循性管理(A.15)
3.強化客戶個人資料安全管理	3.1 客戶資料隱私管理 3.2 客戶資料盤點作業 3.3 客戶資料依法對外公開、資訊揭露作業 3.4 客戶資料蒐集、處理及儲存管理作業 3.5 客戶資料使用及傳輸安全作業 3.6 客戶資料正確性維護作業 3.7 客戶資料刪除及停止利用作業	- 本文(7, 8) - 人員安全管理(A.8) - 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 資訊安全事故管理(A.13) - 營運持續管理(A.14) - 遵循性管理(A.15)
4.提升企業內資訊環境安全管理	4.1 網路通訊與資訊作業安全管理 4.2 電子郵件安全管理 4.3 個人資訊設備安全管理 4.4 網際網路內容瀏覽管理	- 組織管理(A.6) - 資產管理(A.7) - 人員安全管理(A.8) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 遵循性管理(A.15)

策略目標	管理項目	ISO 27001 管理領域對照
5. 強化對外網站交易平台安全管理	5.1 客戶隱私保護政策宣告作業 5.2 交易網站伺服器與網路環境安全管理 5.3 線上交易安全管理 5.4 交易網站技術弱點管理	- 本文(7.1) - 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 資訊安全事故管理(A.13) - 營運持續管理(A.14) - 遵循性管理(A.15)
6. 建立資安通報管理機制	6.1 電子商務資安通報機制 6.2 資安事故管理	- 資訊安全事故管理(A.13)

資料來源：本計畫整理

表 6　網路平台交易安全規範與個資法施行細則草案符合性對照

個資法施行細則第九條	管理項目	查檢項目	重點說明	因應對策	參與單位
一、成立管理組織，配置相當資源。	3.1 客戶資料隱私管理	3.1.2	1. 成立管理組織 2. 配置相當資源 3. 個資安全維護組織運作	成立管理組織，配置相當資源	- 公司高層 - 負責個資安全維護組織 - 個資處理專職 - 稽核部門與法務
二、界定個人資料之範圍。	3.2 客戶資料盤點作業	3.2.1	1. 個人資料定義 2. 個人資料盤點 3. 個人資料管理權責規劃	界定個人資料之範圍	- 資訊部門 - 個資處理專職 - 稽核部門與法務
三、個人資料之風險評估及管理機制。	3.1 客戶資料隱私管理	3.1.4	1. 個人資料隱私衝擊分析 2. 個人資料之風險評估 3. 個人資料	個人資料之風險評估及管理機制	- 公司高層 - 資訊部門 - 個資處理專職 - 稽核部

個資法施行細則第九條	管理項目	查檢項目	重點說明	因應對策	參與單位
			之風險管理機制		門與法務
四、事故之預防、通報及應變機制。	3.1 客戶資料隱私管理	3.1.3	1. 事故之預防 2. 事故之通報 3. 事故應變機制	事故之預防、通報及應變機制	- 資訊部門 - 個資處理專職 - 稽核部門與法務
五、個人資料蒐集、處理及利用之內部管理程序。	3.4 客戶資料蒐集、處理及儲存管理作業	3.4.1 3.4.2 3.4.3 3.4.4 3.4.5	1. 個人資料蒐集流程管理 2. 個人資料處理流程管理 3. 個人資料利用流程管理	個人資料蒐集、處理及利用之內部管理程序	- 資訊部門 - 個資處理專職 - 稽核部門與法務
六、資料安全管理及人員管理。	3.5 客戶資料使用及傳輸安全作業	3.5.3	1. 資料安全管理 2. 內部人員管理 3. 第三方受託機關人員管理	資料安全管理及人員管理	- 資訊部門 - 個資處理專職 - 人資部門 - 稽核部門與法務
七、認知宣導及教育訓練。			1. 認知宣導 2. 教育訓練	認知宣導及教育訓練	- 資訊部門 - 個資處理專職 - 人資部門 - 稽核部門與法務
八、設備安全管理。	3.4 客戶資料蒐集、處理及儲存管理作業	3.4.5	1. 實體與環境安全管理 2. 儲存設備安全管理 3. 傳輸設備安全管理	個資法防護方案及設備安全管理	- 資訊部門 - 稽核部門
九、資料安全稽核機制。	3.4 客戶資料蒐集、處理及	3.4.4	1. 內部個資處理流程稽核	資料安全稽核機制包含但不	- 資訊部門 - 稽核部門

個資法施行細則第九條	管理項目	查檢項目	重點說明	因應對策	參與單位
	儲存管理作業		2. 內部個資紀錄稽核 3. 部署適當監控工具	限於Email稽核／備份、上網行為管理、資料庫稽核機制、防火牆及資料防漏機制(DLP)	
十、必要之使用紀錄、軌跡資料及證據之保存。	3.4 客戶資料蒐集、處理及儲存管理作業	3.4.5 3.6.1 3.7.3 3.7.4	1. 個資使用紀錄之保存 2. 軌跡資料之保存 3. 證據之保存	必要之使用紀錄軌跡資料及證據之保存，例如Email稽核／備份、稽核紀錄、上網行為管理紀錄、資料庫防火牆紀錄	- 資訊部門 - 稽核部門與法務
十一、個人資料安全維護之整體持續改善。	3.4 客戶資料蒐集、處理及儲存管理作業	3.4.4	1. 定期內部審查 2. 定期個資安全維護組織會議 3. 個資安全維護改善計畫	個人資料安全維護之整體持續改善	- 資訊部門 - 個資處理專職 - 稽核部門與法務

肆、規範內容

說明：

本節為本規範要求項目所有內容，其表列順序依照第參章第一節整體大綱，內容涵括規範之第一層至第三層，並標示每一條規範之適用業者分類類別以及依據之法規或標準名稱。

表 7　網路平台交易安全規範要求項目表

管理項目	要求項目	類別	依據之法規或標準
策略目標：1.促進組織資訊安全管理			
1.1 資訊安全框架	1.1.1 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。	皆適用	ISO 27001
	1.1.2 電子商務網路平台管理階層，應具體說明其對資安之承諾與責任。	皆適用	ISO 27001
1.2 風險管理	1.2.1 電子商務網路平台應分析營運交易之資安風險，分析結果並經管理階層同意。	皆適用	ISO 27001
	1.2.2 電子商務網路平台應針對重大風險，建立並執行具體因應對策。	皆適用	ISO 27001
1.3 資訊資產管理	1.3.1 電子商務網路平台應清查營運範圍內之資訊資產，至少包含營運相關軟硬體、資料、服務與人員等。	皆適用	ISO 27001
	1.3.2 電子商務網路平台應針對營運範圍內之重要資訊資產，建立適當之資產管理機制。	皆適用	ISO 27001
1.4 人力安全管理	1.4.1 電子商務網路平台應針對相關作業人員之可能偏差行為(如資料盜取或操作錯誤)，預先約束與具體控管。	皆適用	ISO 27001
	1.4.2 電子商務網路平台應針對相關作業人員進行資安教育訓練與宣導。	皆適用	ISO 27001
1.5 遵循性管理	1.5.1 電子商務營業應遵守民法、刑法、消保法、公平交易法、智慧財產權與個資法等相關法令法規，並滿足所提供之服務契約要求。	皆適用	ISO 27001
	1.5.2 管理階層應提供預算支援並定期審查，以使電子商務網路平台維運所需之軟體皆符合智慧財產權相	皆適用	ISO 27001

管理項目	要求項目	類別	依據之法規或標準
	關法令法規。		
	1.5.3 管理階層應定期審查，確認電子商務網路平台保存應有的重要系統日誌，確實控管技術相關弱點，以提供法令規定之良善管理佐證資料。	皆適用	ISO 27001
1.6 委外管理	1.6.1 電子商務平台業者之委外合約管理及商業夥伴選擇(包含供應商、賣方廠商、運輸業者、倉儲服務、定點取件服務、金流服務或資訊服務廠商)，應充分考量其資安能力與配合度。	皆適用	ISO 27001
	1.6.2 電子商務業者於委外服務作業中，應確保作業之資訊安全。	皆適用	ISO 27001
	1.6.3 電子商務業者於貨物交遞時，應確保物流配送作業之資訊安全。	皆適用	ISO 27001
	1.6.4 電子商務業者於商品供應商或契約店家之出貨作業，應確保其作業之資訊安全。	皆適用	ISO 27001
策略目標：2. 加強核心營運系統與資料庫之安全管理			
2.1 核心營運系統取得、開發及維護安全管理	2.1.1 電子商務網路平台的新資訊系統或現有資訊系統中，為了保障安全應考量以文件詳述資訊安全之要求。	皆適用	ISO 27001
	2.1.2 輸入核心營運系統的資料應透過程式邏輯設計予以檢查，確保資料正確。	皆適用	ISO 27001
	2.1.3 核心營運系統的作業系統之升級或更新應有適當的管制。	皆適用	ISO 27001
	2.1.4 核心營運系統的測試環境應予以獨立，並避免以真實客戶資料進行。	皆適用	ISO 27001
	2.1.5 核心營運系統的程式碼應僅可由授權管理人員才可存取，並將相關行為予以記錄。	皆適用	ISO 27001
	2.1.6 核心營運系統應於新功能上線或變更時執行測試，測試內容應同時考慮系統功能、可用性及安全性。	皆適用	ISO 27001
2.2 核心營運系統存取控制管理	2.2.1 核心營運系統及其相關網路服務皆應有足夠強度的帳號申請及管理規定，使用者、系統管理者帳號及權限皆應有申請核准紀錄，及離調職時取消帳號紀錄。	皆適用	ISO 27001

管理項目	要求項目	類別	依據之法規或標準
	2.2.2 核心營運系統應有足夠強度的通行碼管理規定，包含通行碼複雜度強制要求、首次登入時變更通行碼、變更時應有身份驗證措施。	皆適用	ISO 27001
	2.2.3 含有客戶個人資料之紙本與可移除式媒體不可置放於桌面，電腦並應設定螢幕保護程式予以鎖定。	皆適用	ISO 27001
	2.2.4 核心營運系統所在之網路應進行網路區隔，並針對連線進行限制。	皆適用	ISO 27001
	2.2.5 核心營運系統之公用程式應用(如遠端連線程式、外部連線存取等)應進行管制。	皆適用	ISO 27001
	2.2.6 核心營運系統之連線時間應進行管制。	皆適用	ISO 27001
2.3 核心營運系統機房與作業環境實體安全	2.3.1 應確保重要資料處理及辦公區域之實體安全，避免竊盜或損害。	皆適用	ISO 27001
	2.3.2 應確保核心營運系統機房之實體安全，避免竊盜或損害。	皆適用	ISO 27001
	2.3.3 核心營運系統機房與辦公區域外之設備應設計安全措施，保護場所管控外設備之安全。	皆適用	ISO 27001
	2.3.4 設備外送或淘汰前應進行安全措施，防止資訊外洩。	皆適用	ISO 27001
2.4 核心營運系統資料庫安全管理	2.4.1 核心營運系統的資料庫應建立連線管制與存取控制機制，以保護消費者資料與交易資訊。	皆適用	ISO 27001
	2.4.2 核心營運系統的資料庫應定期查檢，以保護消費者資料與交易資訊之正確與完整。	皆適用	ISO 27001
	2.4.3 核心營運系統之資料庫應定期備份。	皆適用	ISO 27001
	2.4.4 核心營運系統之資料庫應留存重要存取紀錄。	皆適用	ISO 27001
2.5 核心營運系統營運持續安全管理	2.5.1 電子商務核心流程應訂定能確保及時復原必要運作之營運持續計畫。	皆適用	ISO 27001
策略目標：3. 強化客戶個人資料安全管理			
3.1 客戶資料隱私管理	3.1.1 應於網站或公司營運據點所屬範圍之適當地點公告隱私權保護宣告或政策，相關資訊至少包含客戶資料蒐集與利用範圍、第三方協同作業範圍、資料保護安全措施等。	皆適用	「個人資料保護法」

管理項目	要求項目	類別	依據之法規或標準
	3.1.2 應成立管理組織並依作業需求指定作業人員之權責，以依相關法令辦理安全維護及客戶個人資料保管事項。	皆適用	「個人資料保護法」
	3.1.3 應設置並對外公告「客戶個人資料保護聯絡窗口」，協調聯繫客戶資料事宜，及擔任消費者提出申訴與救濟時之單一窗口。	皆適用	「個人資料保護法」
	3.1.4 應辨識電子商務營運流程中，「客戶個人資料保護」可能遭遇的重大風險(如駭客入侵竊取個資等)，建立並執行具體因應對策。	皆適用	ISO 27001
3.2 客戶資料盤點作業	3.2.1 應定期盤點電子商務營運服務流程(包含輸入與輸出)所涉及的客戶個人資料之敏感等級、儲存使用方式、傳輸媒介、接觸人員等，並評估其相對應的安全維護措施之強度。	皆適用	「個人資料保護法」
3.3 客戶資料依法對外公開、資訊揭露作業	3.3.1 應依據法律規定、契約及正式對外宣告之隱私權政策，並於蒐集時即告知客戶相關訊息，始得執行客戶個人資料對外公開、資訊揭露等作業。	皆適用	「個人資料保護法」
	3.3.2 所訂定之「客戶個人資料保護政策與程序」應包含所有線上及離線作業，明確規定客戶資料對外公開、資訊揭露作業之期間、地區、對象、處理方式與保護範圍(界定交易網頁由平台業者或委外第三方單位控管)。	皆適用	「個人資料保護法」
3.4 客戶資料蒐集、處理及儲存管理作業	3.4.1 蒐集、處理或利用客戶個人資料時，應依照法令規定，透過文字描述其合理關連之特定目的、使用方式及消費者個人資料相關權利之行使方式，並取得當事人同意。	皆適用	「個人資料保護法」
	3.4.2 應對保有客戶個人資料之部門員工宣導與規範禁止向任何未經授權的第三人交付、揭露、出售或轉讓所蒐集之個人資料，並認知其保護個資之職責。	皆適用	「個人資料保護法」
	3.4.3 應於向三方揭露或由委外廠商處理客戶個人資料前，確保其合法性並取得對客戶個人資料安全保護之能力與承諾。	皆適用	「個人資料保護法」
	3.4.4 客戶個人資料之處理行為應經權責單位核准，並訂定個人資料管理之稽核程序及設置稽核人員以定期審查作業情形並留存相關稽核紀錄。	皆適用	「個人資料保護法」、ISO 27001

管理項目	要求項目	類別	依據之法規或標準
	3.4.5 存放客戶個人資料檔案(含數位與紙本檔案)之主機、週邊設備及相關設施等，應置於內部至少第二層門禁管制之安全作業區域(或上鎖檔案櫃)，建立完整管理監督程序並留存相關紀錄。	皆適用	ISO 27001
3.5 客戶資料使用及傳輸安全作業	3.5.1 客戶個人資料之使用、傳遞與交換作業等相關資訊，應於蒐集當時、變更時告知並取得當事人同意。	皆適用	「個人資料保護法」
	3.5.2 需以企業網路與外部廠商或客戶交換之資料，應有適當加密或其他保全機制，不得明碼傳送。	皆適用	「個人資料保護法」
	3.5.3 客戶個人資料之使用、傳遞與交換作業(包含國際傳輸)，應有安全的作業機制，明確規定執行作業之期間、地區、對象、申請及處理方式，並留存定期查檢紀錄。	皆適用	「個人資料保護法」、ISO 27001
3.6 客戶資料正確性維護作業	3.6.1 應訂定有明確作業步驟與作業周期性以更新、維護客戶個人資料，於必要時應及時更新，並留下相關作業查核紀錄。	皆適用	「個人資料保護法」
	3.6.2 應對客戶提出其個人資料諮詢、更新與申訴等服務時，有完整的執行步驟與客戶回應說明。	皆適用	「個人資料保護法」
	3.6.3 利用電腦處理客戶個人資料時，應有內部作業查驗程序，以確保輸入資料與原資料相符合。	皆適用	「個人資料保護法」、ISO 27001
	3.6.4 客戶欲維護個人資料之正確性或發生爭議時，尊重消費者權益與意願，立即停止處理或利用，並於30日內予以回應處理狀況。	皆適用	「個人資料保護法」
3.7 客戶資料刪除及停止利用作業	3.7.1 含有客戶資料之儲存媒體之汰除，應使用格式化或其他實體破壞方式予以銷毀。	皆適用	「個人資料保護法」
	3.7.2 應每日檢查環境周遭是否有未妥善保管之客戶資料。	皆適用	「個人資料保護法」、ISO 27001
	3.7.3 欲廢棄或不再持有之客戶紙本資料，應使用碎紙機或其他實體破壞方式予以確實銷毀，或委由專業處理廠商於專人監督下銷毀。	皆適用	「個人資料保護法」、ISO 27001

管理項目	要求項目	類別	依據之法規或標準
	3.7.4 應控管電子客戶個人資料留存的時間，定期由專人或負責人員刪除，並由主管不定期抽檢。	皆適用	「個人資料保護法」、ISO 27001
策略目標：4. 提升企業內資訊環境安全管理			
4.1 網路通訊與資訊作業安全管理	4.1.1 重要資訊設備與通訊設施管理人員應熟悉操作程序，於設定變更異動設備時應留存相關核准與測試紀錄。	皆適用	ISO 27001
	4.1.2 含有客戶個資之重要作業職權應加以區隔，以降低資產遭未經授權或非意圖的修改或誤用之機會。	皆適用	ISO 27001
	4.1.3 應安裝防毒軟體，並定期更新病毒碼及執行系統掃描作業。	皆適用	ISO 27001
	4.1.4 重要資料及資訊系統應定期進行系統與軟體的備份與還原測試。	皆適用	ISO 27001
	4.1.5 應定期檢測網路安全及連線品質，以確保網路的系統與應用程式的安全。	皆適用	ISO 27001
	4.1.6 應安裝防火牆或入侵偵測系統，定期檢查防火牆和路由器的規則設定，以保護系統之安全。	皆適用	ISO 27001
	4.1.7 記錄使用者活動、異常及資訊安全事件，宜產生與保留一段議定的期間，以協助未來的調查與存取控制監視。	皆適用	ISO 27001
	4.1.8 所有交易相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。	皆適用	ISO 27001
4.2 電子郵件安全管理	4.2.1 應制定電子郵件使用規則，以維護使用郵件的系統與應用程式的安全。	皆適用	ISO 27001
	4.2.2 應訂定執行電子商務作業之電子郵件帳號申請、密碼設定要求等管理規則。	皆適用	ISO 27001
	4.2.3 應設置防止垃圾郵件或設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件。	皆適用	ISO 27001
4.3 個人資訊設備安全管理	4.3.1 應定期進行系統更新，以避免遭受弱點攻擊。	皆適用	ISO 27001
	4.3.2 應制定使用者電腦使用管理規範，要求使用者通行碼、電腦使用、資訊設備操作及工作行為需注意事項。	皆適用	ISO 27001

管理項目	要求項目	類別	依據之法規或標準
4.4 網際網路內容瀏覽管理	4.4.1 應建立網路路由控制，以確保電腦連線與資訊流未違反應用系統之存取控制政策。	皆適用	ISO 27001
	4.4.2 應限制高風險業務或敏感性資訊避免使用即時通訊軟體或外部電子郵件信箱進行資料傳輸作業。	皆適用	ISO 27001
策略目標：5. 強化對外網站交易平台安全管理			
5.1 客戶隱私保護政策宣告作業	5.1.1 應至少每年審查一次對外公告之隱私權政策，並向所有消費者發布。	皆適用	「個人資料保護法」、ISO 27001
5.2 交易網站伺服器與網路環境安全管理	5.2.1 應監視、調諧網路流量、硬碟空間等系統容量的使用與網路連線之狀態，並對未來容量要求預作規劃，以確保所要求之效能。	皆適用	ISO 27001
	5.2.2 對外交易網站之網路安全維護上應考量建立連線限制與網路區隔，並架設防火牆或入侵偵測系統。	皆適用	ISO 27001
	5.2.3 電子商務線上交易程式或涉及金流與交易相關的應用程式開發，應遵循「2.1 核心營運系統取得、開發及維護安全管理」各項規範要求。	皆適用	ISO 27001
	5.2.4 應設定交易頁面之瀏覽、讀取等限制設定，禁止目錄瀏覽及切換目錄，避免網站目錄內檔案遭竄改或變更。	皆適用	ISO 27001
	5.2.5 應對交易網站所涉及的各項機敏性資料，制定必要的管控政策與措施。	皆適用	ISO 27001
5.3 線上交易安全管理	5.3.1 應有網站交易使用者之帳號管理安全機制，如進行使用者身分認證、強制要求帳號密碼強度等，並記錄帳號申請之核准和撤銷。	皆適用	ISO 27001
	5.3.2 電子商務交易系統應加入查核機制，以預防因作業處理疏失或故意行為所導致之線上交易資訊異常。	皆適用	ISO 27001、「消費者保護法」
	5.3.3 應透過適當之控管措施與安全連線機制(如 SSL 加密等方法)進行交易資料之傳送與傳輸(含資料往返、互換及二次以上傳遞)，以防止未經授權的存取。	皆適用	ISO 27001
	5.3.4 敏感性資料(如身份證字號、信用卡卡號等資訊)於交易畫面顯示時，應遮蔽並透過加密機制傳輸，避免資料遭竊取。	皆適用	ISO 27001

管理項目	要求項目	類別	依據之法規或標準
	5.3.5 應透過密碼、檔案加密工具或金鑰針對儲存之交易資料進行加密。	皆適用	ISO 27001
	5.3.6 交易資料庫應禁止留存客戶信用卡卡號、驗證碼，並不將個人資料等敏感訊息存於公開之網頁伺服器。	皆適用	ISO 27001
	5.3.7 應留存對外交易網站之交易與信用卡資料存取交易紀錄，並定期審查交易網站相關設備(含主機、網路設備、資料庫等)之日誌資訊。	皆適用	ISO 27001
5.4 交易網站技術弱點管理	5.4.1 對外交易網站應修改預設參數，並建立網站攻擊手法之預防機制。	皆適用	ISO 27001
	5.4.2 對外交易網站應定期實施各式技術性弱點測試，以強化電子商務交易服務安全。	皆適用	ISO 27001
策略目標：6. 建立資安通報管理機制			
6.1 電子商務資安通報機制	6.1.1 電子商務網路平台應參照電子商務資安通報機制規範，進行資安事故外部通報。	皆適用	ISO 27001
6.2 資安事故管理	6.2.1 應建立資安事故通報管理程序，並對內外部員工宣導相關通報流程。	皆適用	ISO 27001
	6.2.2 應界定人員緊急應變的責任，以確保對資訊安全事故做迅速、有效及依序的回應。	皆適用	ISO 27001
	6.2.3 應收集、保存及呈現資安事故之完整證據，並針對事故之原因進行檢討分析。	皆適用	ISO 27001

資料來源：本計畫整理

伍、規範查檢表

說明：

(一) 查檢表格式依循規範大綱及管理項目，分別制定要求之查檢項目與對應之檢核方法。

(二) 類別欄位標示“皆適用”者，表示第一、二類業者皆適用；標示“II”表示僅第二類業者適用。

(三) 進階指引欄位標示“◎”表示為進階指引(Better Practices)之參考項目，可依據風險管理需求選擇性執行；未標示者表示該查檢項目為應執行之作業基準(Baselines)，業者應落實執行。

(四) 檢核結果欄位，提供業者自我查核或第三方查核時，針對該查檢項目之查核結果，記錄執行現況是否符合要求。進階指引項目於查核前，應先辨識該項目是否適用，經辨識為不適用項目者，毋須再做檢核紀錄。

(五) 檢核紀錄欄位，提供業者自我查核或第三方查核時，針對該查檢項目之執行現況予以記錄。該欄位已列出之相關紀錄確認，為提供業者實施本規範之操作面參考，非為執行限制，故檢核紀錄可增列所有實際檢核之佐證資訊。

表 8　規範查檢表

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1. 促進組織資訊安全管理					
1.1 資訊安全框架					
1.1.1 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。					
1.1.1.1	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)？			□ 適用 □ 不適用 說明：	□ 制定政策，內容包含： - 資訊安全的目標

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					- 概要資訊安全原則的需求 - 公司內部權責 ☐ 政策公告內部員工 ☐ 政策公告給外部廠商 ☐ 政策定期審查與更新
1.1.1.2	是否建立資訊安全相關文件及其紀錄之管理與管制程序？		◎	☐ 適用 ☐ 不適用 說明：	
1.1.1.3	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？			☐ 適用 ☐ 不適用 說明：	☐ 訂有資安內部稽核計畫 ☐ 定期辦理資安內部稽核
1.1.1.4	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)？			☐ 適用 ☐ 不適用 說明：	☐ 產生稽核報告 ☐ 追踪改善情形
1.1.1.5	內部稽核範圍是否考量涵蓋供應商、物流商、產業供應鏈其他業者？		◎	☐ 適用 ☐ 不適用 說明：	
1.1.1.6	是否針對資訊安全之落實，定期進行量測與比較，確保其有效性？		◎	☐ 適用 ☐ 不適用 說明：	
1.1.2 電子商務網路平台管理階層，應具體說明其對資安之承諾與責任。					
1.1.2.1	高階管理階層是否制定、審查及核准資訊安全實作？			☐ 適用 ☐ 不適用 說明：	
1.1.2.2	是否指派適當權責之管理階層或成立跨部門單位負責推動、協調及監督資訊安全管理事項？		◎	☐ 適用 ☐ 不適用 說明：	☐ 指派特定管理階層 ☐ 成立跨部門資安小組
1.1.2.3	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？			☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.1.2.4	資訊安全責任的配置是否依據資訊安全政策，明確識別保護個別資產與執行特定安全作業過程的責任並予以書面化？		◎	□ 適用 □ 不適用 說明：	□ 書面訂定資安權責分配
1.1.2.5	是否依據員工之職務內容，訂定員工資訊安全作業程序、權責規範或授權層級並予以書面化？(含經管使用設備與相關作業須知)		◎	□ 適用 □ 不適用 說明：	□ 書面訂定員工資訊安全作業程序
1.1.2.6	是否訂定各項資訊處理設施之用途及使用授權，以及其安全之作業程序？		◎	□ 適用 □ 不適用 說明：	□ 書面訂定資訊處理設施之用途及使用授權
1.1.2.7	如使用筆記型電腦、家用電腦或手持裝置等個人或私人擁有的資訊處理設施來處理營運資訊，是否識別並實作必要的各項控制措施？		◎	□ 適用 □ 不適用 說明：	
1.1.2.8	是否依據資訊設備、安全區域及資訊的機密性，制定其保密協議？		◎	□ 適用 □ 不適用 說明：	
1.1.2.9	當有已法規遵循之疑慮時，是否備有及時與權責機關聯繫、通報(例如：執法機關、消防單位及事業主管機關)所識別的資訊安全事故之適當程序或規定 ？			□ 適用 □ 不適用 說明：	
1.1.2.10	是否訂定與各特殊利害相關團體、專家安全性論壇、及專業協會聯繫管道？		◎	□ 適用 □ 不適用 說明：	
1.1.2.11	是否定期或當資安作業環境發生重大變更時，由管理階層召開審查會議，獨立審查組織對管理資訊安全的作法與其實作(例如：各項資訊安全的控制目標、控制措施、政策、過程及程序)？			□ 適用 □ 不適用 說明：	□ 定期召開資安管理審查會議並留有會議紀錄 □ 召開管理審查會議審查重大變更(如：機房搬遷)
1.2 風險管理					
1.2.1 電子商務網路平台應分析營運交易之資安風險，分析結果並經管理階層同意。					
1.2.1.1	是否利用特定方法，定期對企業之資訊資產進行風險評鑑，識別特定風險與層級，並予以重視處理之？		◎	□ 適用 □ 不適用 說明：	□ 至少每年一次以上
1.2.1.2	是否指定專人或專責單位辦理風險評鑑、資訊分類、系統安全控管措施？		◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.2.1.3	是否鑑別適用範圍內之所有資訊資產及其擁有者？		◎	□ 適用 □ 不適用 說明：	
1.2.1.4	是否定義風險評鑑的特定方法，且該方法可產出可比較與可再產生之結果？		◎	□ 適用 □ 不適用 說明：	
1.2.1.5	是否鑑別所有資產可能遭遇之威脅？			□ 適用 □ 不適用 說明：	□ 書面列出所有資產之威脅
1.2.1.6	是否鑑別所有資產可能之脆弱點？			□ 適用 □ 不適用 說明：	□ 書面列出所有資產之脆弱點
1.2.1.7	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？			□ 適用 □ 不適用 說明：	□ 書面列出資產可能之威脅
1.2.1.8	是否評鑑因發生安全事件而可能對公司造成之傷害及產生之後果？			□ 適用 □ 不適用 說明：	
1.2.1.9	是否評鑑安全事件發生之可能性或機率？		◎	□ 適用 □ 不適用 說明：	
1.2.1.10	是否評鑑所有資產可能發生之風險值？		◎	□ 適用 □ 不適用 說明：	
1.2.1.11	公司是否確定風險接受水準與可接受風險之等級，並皆由管理階層核定之？		◎	□ 適用 □ 不適用 說明：	
1.2.2 電子商務網路平台應針對重大風險，建立並執行具體因應對策。					
1.2.2.1	對於需要控管之風險是否依其重要性決定其處理之優先順序？		◎	□ 適用 □ 不適用 說明：	
1.2.2.2	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？			□ 適用 □ 不適用 說明：	□ 書面訂定風險處理計畫 □ 確認導入控制措施
1.2.2.3	是否有書面化的持續進行風險管理之記錄？		◎	□ 適用 □ 不適用 說明：	□ 書面的風險評鑑方法論 □ 書面的風險評鑑報告及風險處理計畫 □ 定期進行風險再評

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					鑑紀錄
1.3 資訊資產管理					
1.3.1 電子商務網路平台應清查營運範圍內之資訊資產，至少包含營運相關軟硬體、資料、服務與人員等。					
1.3.1.1	新購置與租賃之資訊設備，是否依照公司採購相關管理程序之驗收流程進行驗收，並會簽資訊部門進行必要之安全檢核，始可上線使用？			□ 適用 □ 不適用 說明：	□ 建立營運範圍之重要資產清冊
1.3.1.2	資產清冊是否定期審查，確保其隨時更新且處於適切狀態？			□ 適用 □ 不適用 說明：	□ 定期更新資產清冊
1.3.2 電子商務網路平台應針對營運範圍內之重要資訊資產，建立適當之資產管理機制。					
1.3.2.1	是否識別所有資訊資產之擁有者，並指派維護資訊資產之適切控制措施的責任？			□ 適用 □ 不適用 說明：	□ 指派資訊資產之擁有者
1.3.2.2	是否識別及實作所有資訊處理設施相關的資訊與資產(含電子郵件、網路使用及行動設備等)之使用規則並文件化？		◎	□ 適用 □ 不適用 說明：	
1.3.2.3	新購置與租賃之資訊設備，是否依照公司採購相關管理程序之驗收流程進行驗收，並會簽資訊部門進行必要之安全檢核，始可上線使用？			□ 適用 □ 不適用 說明：	□ 設備由權責單位進行驗收 □ 設備經過資訊安全檢查程序
1.3.2.4	是否依據資訊資產對公司的價值、法律要求、敏感性及重要性等項目加以分類？		◎	□ 適用 □ 不適用 說明：	
1.3.2.5	是否依據公司採用的分類原則與方法，制定適當之資訊標示與處置方式？		◎	□ 適用 □ 不適用 說明：	
1.3.2.6	對於敏感或關鍵之資訊，是否附上適當的分類標籤或標示？		◎	□ 適用 □ 不適用 說明：	
1.3.2.7	若屬機密性、敏感性之手稿、影印廢紙及已過法律保存期限之留存文件，棄置之前是否予以銷毀？			□ 適用 □ 不適用 說明：	□ 採用碎紙機銷毀 □ 未有棄置未管理之機敏文件

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.4 人力安全管理					
1.4.1 電子商務網路平台應針對相關作業人員之可能偏差行為(如資料盜取或操作錯誤)，預先約束與具體控管。					
1.4.1.1	是否依照公司的資訊安全政策，界定與文件化所有員工、產業供應鏈上下游業者或第三方使用者之安全角色與責任，包括關於機密性、資料保護、及適切使用公司設備與設施？		◎	□ 適用 □ 不適用 說明：	□ 簽訂保密切結與載明保密協議 □ 訂有資安查核或委託第三方查核之權利
1.4.1.2	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？			□ 適用 □ 不適用 說明：	□ 程式開發與資料庫管理權限予以分散
1.4.1.3	是否詳細檢查職務能合法存取關鍵服務、客戶資訊，客戶要求的內容已納入相關安全責任？		◎	□ 適用 □ 不適用 說明：	
1.4.1.4	是否明確定義背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及聘僱相關法令？		◎	□ 適用 □ 不適用 說明：	
1.4.1.5	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？			□ 適用 □ 不適用 說明：	□ 員工已簽署保密協議 □ 外部廠商已簽署保密協議
1.4.1.6	是否訂有員工違反公司安全政策與程序之懲處規定？		◎	□ 適用 □ 不適用 說明：	
1.4.2 電子商務網路平台應針對相關作業人員進行資安教育訓練與宣導。					
1.4.2.1	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？			□ 適用 □ 不適用 說明：	□ 管理階層以公告或宣導之任何方式要求依程序執行安全事宜 □ 明確說明並公告資安責任 □ 告知內部員工 □ 告知外部廠商
1.4.2.2	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			□ 適用 □ 不適用 說明：	□ 施行資安教育訓練並留存訓練紀錄 □ 內部員工參與 □ 外部廠商參與

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	練？				
1.4.2.3	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產？(包含歸還所有先前發出的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他公司資產)			□ 適用 □ 不適用 說明：	
1.4.2.4	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？			□ 適用 □ 不適用 說明：	
1.4.2.5	是否對人員晉用考量相關資訊證照或適當的電子商務知識和技能？		◎	□ 適用 □ 不適用 說明：	
1.4.2.6	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？			□ 適用 □ 不適用 說明：	□ 施行客戶隱私保護相關教育訓練 □ 訂定宣導文件並公告公司內部員工與外部廠商
1.5 遵循性管理					
1.5.1 電子商務營業應遵守民法、刑法、消保法、公平交易法、智慧財產權與個資法等相關法令法規，並滿足所提供之服務契約要求。					
1.5.1.1	是否要求所有資訊系統、公司及產業供應鏈業者均不違反任何法律、法令、法規或契約義務，以及任何安全要求？			□ 適用 □ 不適用 說明：	□ 委外合約之保密協議 □ 委外合約之服務保證條款 □ 委外合約之智慧財產權歸屬
1.5.1.2	是否發展和實作符合法律、法規及若適用的契約條文所要求的資料保護與隱私政策？		◎	□ 適用 □ 不適用 說明：	
1.5.1.3	公司以及產業供應鏈業者中對於所經管或處理之資訊，涉有個人隱私及個人資料之保護是否有妥適之保護機制？		◎	□ 適用 □ 不適用 說明：	□ 委外合約之客戶個人資料保護要求與聲明

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.5.1.4	管理人員是否定期審查其責任範圍內的資訊處理設施與其安全政策、標準及其他任何安全要求的遵循性？		◎	□ 適用 □ 不適用 說明：	
1.5.2 管理階層應提供預算支援並定期審查，以使電子商務網路平台維運所需之軟體皆符合智慧財產權相關法令法規。					
1.5.2.1	是否維護使用版權、原版光碟片、手冊等所有權的證明和證據，並定期檢核是否只安裝經合法授權軟體與有使用版權的產品？		◎	□ 適用 □ 不適用 說明：	
1.5.2.2	軟體取得(含自行開發、委外開發、購置或租用)等可能涉及智慧財產權規定或合約要求是否可遵循法律、法規及契約的要求？			□ 適用 □ 不適用 說明：	
1.5.2.3	是否公布智慧財產權遵循政策，定義軟體與資訊產品的合法使用，並通知違反政策人員將遭懲處？		◎	□ 適用 □ 不適用 說明：	
1.5.3 管理階層應定期審查，確認電子商務網路平台保存應有的重要系統日誌，確實控管技術相關弱點，以提供法令規定之良善管理佐證資料。					
1.5.3.1	公司重要紀錄(如資料庫紀錄、系統日誌、操作日誌、稽核日誌)是否依安全需要加以保護儲存(如檔案加密或數位簽章)？		◎	□ 適用 □ 不適用 說明：	
1.5.3.2	是否有監控設備或其他可偵測未經授權使用的設備，以防止資訊設施被不當使用？		◎	□ 適用 □ 不適用 說明：	
1.5.3.3	是否要求軟體開發人員，程式上線前須通過白箱安全檢測？		◎	□ 適用 □ 不適用 說明：	
1.5.3.4	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。			□ 適用 □ 不適用 說明：	□ 已更新作業系統漏洞 □ 已更新作業軟體漏洞
1.5.3.5	核心營運系統是否定期進行技術層面安全符合性之檢查(如實作滲透測試、入侵偵測或系統弱點檢測)？		◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.5.3.6	技術遵循性查核人員是否經過訓練，並作事前工作分配？			□ 適用 □ 不適用 說明：	□ 查核人員經過教育訓練或通過適當查核證照 □ 查核團隊已訂定查核計畫並分配工作
1.5.3.7	技術遵循性檢查是否由合格資安技術單位執行？		◎	□ 適用 □ 不適用 說明：	
1.5.3.8	技術遵循性查核之執行是否有適當的管控以避免相關安全疑慮？		◎	□ 適用 □ 不適用 說明：	□ 技術遵循性查核結果的文件化紀錄 □ 查核時的存取行為之紀錄(包含查核時的管控或監測紀錄)
1.6 委外管理					
1.6.1 電子商務平台業者之委外合約管理及商業夥伴選擇(包含供應商、賣方廠商、運輸業者、倉儲服務、定點取件服務、金流服務或資訊服務廠商)，應充分考量其資安能力與配合度。					
1.6.1.1	基於供應鏈安全之考量，選擇商業夥伴，包含供應商、賣方廠商、運輸業者、倉儲服務、定點取件服務、金流服務或資訊服務廠商，是否具有書面且可供驗證之程序？		◎	□ 適用 □ 不適用 說明：	
1.6.1.2	選擇服務供應商前，是否進行服務供應商之資訊安全風險評估程序？(例如是否已通過具有公信力之 PDCA 資訊安全管理制度驗證？要求檢視其資訊安全 ISO 27001 之認證影本，以證明該商業夥伴已取得之資訊安全認證範圍包含其提供之主要服務流程或業務)		◎	□ 適用 □ 不適用 說明：	□ 供應商的 ISO 27001 或 PCIDSS 驗證證明文件
1.6.1.3	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。			□ 適用 □ 不適用 說明：	□ 針對服務供應商進行評估並留存書面紀錄

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.6.1.4	委外服務廠商之資訊安全聲明中是否包含應瞭解並確實遵守政府、主管機關等之相關資訊安全法令規定，若有違反願配合公司進行調查？		◎	□ 適用 □ 不適用 說明：	
1.6.1.5	若委外廠商將與公司有關之作業再委外，是否以書面方式知會並取得同意後使進行？公司或委外廠商是否對轉包之再委外單位、人員、資訊實施必要之管制與監控？		◎	□ 適用 □ 不適用 說明：	
1.6.1.6	是否要求委外服務廠商因應公司之稽核需要，配合提供資訊安全管理現況資料，並協助公司人員進行稽核作業？		◎	□ 適用 □ 不適用 說明：	□ 訂有資安查核或委託第三方查核之權利 □ 第三方提供服務期間，定期對提供之服務、報告及紀錄等進行適當之監視與審查，並定期執行稽核之紀錄
1.6.1.7	是否依風險狀況，定期檢視商業夥伴之資訊安全作業程序及設備(必要時於合約訂定稽核訪視的權利)，並確保其資訊安全基準符合要求？		◎	□ 適用 □ 不適用 說明：	
1.6.1.8	是否與第三方資訊委外服務廠商簽訂適當服務定義及交付等級，並賦予相關的安全管理責任，且納入契約條款？		◎	□ 適用 □ 不適用 說明：	□ 與外部廠商簽訂服務等級協定 □ 與外部廠商簽訂安全管理責任
1.6.1.9	由第三方提供之服務如有任何異動時，是否評估資安措施之有效性並作必要之調整？		◎	□ 適用 □ 不適用 說明：	
1.6.1.10	與委外服務廠商簽訂合約時，內容是否至少包含但不限於下列精神之保密敘述： (1) 對於公司之客戶資料負絕對之保密義務及保管責任，未經本公司同意，絕不以任何方式將其洩露、告知、交付予任何第三人，若有違反以致公司遭受損害，合約廠商應同意無條件賠償本公司所受之一			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	切損害(包括訴訟上及非訴訟上之損害)。 (2) 另如涉有民刑事責任，合約廠商並應負起相關所有民刑事責任。				
1.6.1.11	因營運需要開放給產業供應鏈(含物流業者、金流業者、供應商、其他資訊服務廠商、臨僱人員與消費者等)使用之資訊，是否予以識別，並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？		◎	□ 適用 □ 不適用 說明：	
1.6.1.12	1.6.1.12 與委外服務廠商簽訂合約時，內容是否至少包含但不限於下列精神之保密敘述： (1) 對於公司之客戶資料負絕對之保密義務及保管責任，未經本公司同意，絕不以任何方式將其洩露、告知、交付予任何第三人，若有違反以致公司遭受損害，合約廠商應同意無條件賠償本公司所受之一切損害(包括訴訟上及非訴訟上之損害)。 (2)實際作業與處理人員應簽訂個人保密切結書。 (3)另如涉有民刑事責任，合約廠商並應負起相關所有民刑事責任。		◎	□ 適用 □ 不適用 說明：	□ 合約列有相關保密條款 □ 合約針對機敏性資料交換，制定交換協議如：資料交換目的、交換方式、可交換之類別、限制交換後資料之用途，並負有保密義務等。
1.6.2 電子商務業者於委外服務作業中，應確保作業之資訊安全。					
1.6.2.1	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？			□ 適用 □ 不適用 說明：	
1.6.2.2	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？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.6.2.3	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。			□ 適用 □ 不適用 說明：	□ 委外廠商未擁有營運系統或客戶資料之存取權限 □ 委外廠商擁有部分營運系統或客戶資料之存取權限須經正式申請程序
1.6.2.4	委外廠商取得敏感資料前，是否由該委外廠商合約之簽訂單位負責過濾，並列入查核重點？		◎	□ 適用 □ 不適用 說明：	□ 有對委外廠商負責重要文件內容是否包括但不限於以下各項之紀錄：客戶消費模式或使用習性分析；為促銷、抽獎等活動所執行之客戶資料收集與後續獎項寄送等活動之儲存、複製、傳遞運送、銷毀等事項 □ 選商階段或承接業務後接受資訊安全查核單位不定期抽檢紀錄
1.6.2.5	委外廠商若有存取營運系統之行為，是否將記錄重要系統中所有存取及操作的紀錄及其相關儲存規則，列入系統需求規範中？			□ 適用 □ 不適用 說明：	
1.6.2.6	與委外廠商簽訂服務合約之單位，是否同時負責監督委外廠商工作之品質與安全要求？		◎	□ 適用 □ 不適用 說明：	
1.6.2.7	委外廠商及其所屬相關承辦廠商(如上、下游協助廠商)，是否不定期接受安全檢查作業？		◎	□ 適用 □ 不適用 說明：	
1.6.2.8	當與委外廠商之關係中止時(包括到期自然中止與強制中止)，是否將申請其所有的實體與營運系統權限取消？			□ 適用 □ 不適用 說明：	□ 終止合約之廠商未有實體與系統權限
1.6.2.9	因營運需要開放給產業供應鏈(含物流業者、金流業者、供應商、其他資訊服務廠商、臨僱人員與消費		◎	□ 適用 □ 不適用 說明：	□ 限制客戶資料讀取與變更權限 □ 留存存取紀錄

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	者等)使用之資訊,其存取權限是否進行必要的控制措施？並定期審查所有已開放外部使用的存取權限				□ 留存定期審查存取權限之紀錄
1.6.2.10	委外合約廠商作業人員，是否為廠商提供名單內之固定服務人員，並確實穿戴可清楚識別公司之制服、已加蓋合約公司章之識別證(含照片及姓名),或穿戴可辨識身分的裝備，或經由內部陪同人員確認來者後，始可進入公司內部作業？		◎	□ 適用 □ 不適用 說明：	
1.6.2.11	委外廠商欲更換固定作業之人員時，是否於一週前以正式書面、傳真或其他足資識別與確認之方式告知管理單位？			□ 適用 □ 不適用 說明：	
1.6.2.12	是否要求委外廠商傳輸資料過程需加密，有客戶個人資料亦應加密？		◎	□ 適用 □ 不適用 說明：	
1.6.3 電子商務業者於貨物交遞時，應確保物流配送作業之資訊安全。					
1.6.3.1	與物流商簽訂合約時，內容是否至少包含但不限於下列精神之保密敘述： (1) 對於公司之客戶資料負絕對之保密義務及保管責任，未經本公司同意，絕不以任何方式將其洩露、告知、交付予任何第三人，若有違反以致公司遭受損害，合約廠商應同意無條件賠償本公司所受之一切損害(包括訴訟上及非訴訟上之損害)。 (2) 另如涉有民刑事責任，合約廠商並應負起相關所有民刑事責任。			□ 適用 □ 不適用 說明：	□ 合約列有相關保密條款 □ 合約針對機敏性資料交換，制定交換協議如：資料交換目的、交換方式、可交換之類別、限制交換後資料之用途，並負有保密義務等。
1.6.3.2	是否要求物流商定期提供依據商業司「物流商交易安全規範」查檢表之查檢結果，以檢視其遵循規範之符合情形？			□ 適用 □ 不適用 說明：	
1.6.3.3	寄送貨物時，是否確實識別物流廠商符合以下條件之一，方可將寄送物品或郵件交予託送？(1) 合約廠商所提供人員名單內之固定收送			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	件服務人員。(2) 穿戴可辨識身分的裝備。(3) 經由內部作業人員確認來者，並留下相關紀錄。				
1.6.3.4	託運單是否針對除交遞必須之資訊予以適當遮隱，避免出現完整之客戶身分証號、所託運之貨品詳細內容、各種金流交易資訊，與發票相關資料等，以確保客戶隱私?			□ 適用 □ 不適用 說明：	
1.6.3.5	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。			□ 適用 □ 不適用 說明：	
1.6.4 電子商務業者於商品供應商或契約店家之出貨作業，應確保其作業之資訊安全。					
1.6.4.1	與商品供應商或店家簽訂合約時，內容是否至少包含但不限於下列精神之保密敘述： (1) 對於公司之客戶資料負絕對之保密義務及保管責任，未經本公司同意，絕不以任何方式將其洩露、告知、交付予任何第三人，若有違反以致公司遭受損害，合約廠商應同意無條件賠償本公司所受之一切損害(包括訴訟上及非訴訟上之損害)。 (2) 另如涉有民刑事責任，合約廠商並應負起相關所有民刑事責任。			□ 適用 □ 不適用 說明：	
1.6.4.2	是否要求商品供應商或契約店家定期提供依據商業司「供應商交易安全規範」查檢表之查檢結果，以檢視其遵循規範之符合情形？			□ 適用 □ 不適用 說明：	
1.6.4.3	商品供應商與公司進行機敏性資料交換，是否制定交換協議？內容是否包含但不限於以下項目？如：資料交換目的、交換方式、可交換之類別、限制交換後資料之用途，並負有保密義務。			□ 適用 □ 不適用 說明：	
2. 加強核心營運系統與資料庫之安全管理					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1 核心營運系統取得、開發及維護安全管理					
2.1.1 電子商務網路平台的新資訊系統或現有資訊系統中，為了保障安全應考量以文件詳述資訊安全之要求。					
2.1.1.1	建置核心營運系統是否備有系統分析與設計文件？			□ 適用 □ 不適用 說明：	□ 是否備有系統分析文件 □ 是否備有系統設計文件 □ 內容是否至少包含應用系統的流程、架構、初步系統設計、輸出入資料規格、介面設計構想、資料庫架構(Schema)等項目
2.1.1.2	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？			□ 適用 □ 不適用 說明：	□ 遵循特定資安開發標準 □ 驗收時通過弱點掃描 □ 對現有系統運作影響評估
2.1.2 輸入核心營運系統的資料應透過程式邏輯設計予以檢查，確保資料正確。					
2.1.2.1	核心營運系統的輸入資訊是否實作檢查邏輯，以確認其正確與適切性？			□ 適用 □ 不適用 說明：	□ 對字串的輸入加以過濾與限制長度 □ 過濾單、雙引號 □ 針對輸入邏輯進行檢查
2.1.2.2	針對資料欄位的輸入，若為已知之資料範圍，是否提供選單或選項之方式進行輸入？			□ 適用 □ 不適用 說明：	□ 已知資料範圍提供下拉式或點選選單
2.1.2.3	核心營運系統是否針對輸入錯誤，設計各種例外狀況管理(如：擷取和回傳例外狀況、設計例外狀況案例、傳送例外狀況資訊)與處理機制，以擷取與存錄錯誤資訊，防止直接顯示原始完整錯誤資訊給予使用者？		◎	□ 適用 □ 不適用 說明：	
2.1.3 核心營運系統的作業系統之升級或更新應有適當的管制。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1.3.1	核心營運系統之作業系統軟體更新是否需經管理階層授權之人員處理？			□ 適用 □ 不適用 說明：	
2.1.3.2	作業系統若需變更或升級，是否對核心營運系統與軟體作相容性評估？			□ 適用 □ 不適用 說明：	□ 先行於測試機器更新進行軟體相容性評估
2.1.4 核心營運系統的測試環境應予以獨立，並避免以真實客戶資料進行。					
2.1.4.1	核心營運系統測試環境所使用之設備環境是否獨立，不應與提供線上服務之設備環境共用？			□ 適用 □ 不適用 說明：	
2.1.4.2	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？			□ 適用 □ 不適用 說明：	□ 未以真實客戶資料進行 □ 真實客戶資料進行虛擬化 □ 完成測試後移除資料
2.1.5 核心營運系統的程式碼應僅可由授權管理人員才可存取，並將相關行為予以記錄。					
2.1.5.1	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？			□ 適用 □ 不適用 說明：	
2.1.5.2	核心營運系統程式原始碼之存取，是否訂有適當之控制措施？部署安裝後是否管制程式碼？		◎	□ 適用 □ 不適用 說明：	
2.1.5.3	是否針對所有運作中程式原始碼之更新或存取行為留存、維護稽核日誌？		◎	□ 適用 □ 不適用 說明：	
2.1.5.4	針對屬敏感性系統之應用軟體與程式原始碼，是否考量至少保留前三代版本之相關備份？		◎	□ 適用 □ 不適用 說明：	
2.1.6 核心營運系統應於新功能上線或變更時執行測試，測試內容應同時考慮系統功能、可用性及安全性。					
2.1.6.1	是否建立核心營運系統之變更管制程序？		◎	□ 適用 □ 不適用 說明：	□ 留存所有變更紀錄 □ 變更後是否立即更新系統文件
2.1.6.2	核心營運系統變更前後，是否主動公告異動範圍、時間、可能之影響？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1.6.3	核心營運系統變更前是否於測試系統執行緊急復原步驟？			☐ 適用 ☐ 不適用 說明：	☐ 提出緊急復原步驟與計畫 ☐ 事前演練緊急復原步驟
2.1.6.4	是否採用組態管理控制系統來保持所有建置之軟體與文件一致？		◎	☐ 適用 ☐ 不適用 說明：	
2.1.6.5	是否持續觀察系統上線後之狀況，並留存相關紀錄？		◎	☐ 適用 ☐ 不適用 說明：	
2.1.6.6	核心營運系統變更後，是否執行相關安全測試項目已確認應有的安全控管措施與程序仍然有效？		◎	☐ 適用 ☐ 不適用 說明：	☐ 未開啟不必要的服務與通訊埠 ☐ 未開啟不必要的通訊協定 ☐ 未留有不必要的帳號 ☐ 限制以URL直接跳頁瀏覽站內網頁結構 ☐ 防止程式原始碼與錯誤碼暴露過多資訊 ☐ 管理員帳號密碼安全程度符合內部規定 ☐ 輸入欄位已進行測試 ☐ 已執行防駭測試 ☐ 已執行弱點掃描 ☐ 其他原有的安全管制措施仍為有效，如
2.1.6.7	核心營運系統測試作業是否訂立測試計畫並產出測試文件？			☐ 適用 ☐ 不適用 說明：	☐ 訂定測試計畫 ☐ 產出測試報告
2.1.6.8	測試計畫與文件是否至少包含功能測試方式、輸出入介面測試方式、單元測試與整體測試，並依據系統特性，考量增加壓力測試？		◎	☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1.6.9	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)？			□ 適用 □ 不適用 說明：	□ 系統驗收及上線程序 □ 測試報告
2.1.6.10	進行各項核心營運系統漏洞修補前，是否先作系統影響風險評估與測試，再採取必要措施？		◎	□ 適用 □ 不適用 說明：	□ 於測試環境執行漏洞修補測試 □ 洽詢廠商修補之風險
2.2 核心營運系統存取控制管理					
2.2.1 核心營運系統及其相關網路服務皆應有足夠強度的帳號申請及管理規定，使用者、系統管理者帳號及權限皆應有申請核准紀錄，及離調職時取消帳號紀錄。					
2.2.1.1	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？			□ 適用 □ 不適用 說明：	
2.2.1.2	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？			□ 適用 □ 不適用 說明：	
2.2.1.3	是否維持所有使用者註冊服務、系統，或存取資訊等之正式紀錄？		◎	□ 適用 □ 不適用 說明：	
2.2.1.4	基於系統管理或特殊作業需要，如需設定特殊權限時(如系統管理者、高權限之管理者)，是否透過正式的授權過程來控制特權的配置？			□ 適用 □ 不適用 說明：	
2.2.1.5	是否維護所有特權配置(發放、建立特殊權限)的授權過程和紀錄，並於完成正式的授權過程後才授予特權？		◎	□ 適用 □ 不適用 說明：	
2.2.1.6	系統或軟體安裝完畢後，是否立即更新廠商所預設之通行碼？			□ 適用 □ 不適用 說明：	
2.2.2 核心營運系統應有足夠強度的通行碼管理規定，包含通行碼複雜度強制要求、首次登入時變更通行碼、變更時應有身份驗證措施。					
2.2.2.1	核心營運系統使用者是否均有唯一的使用者識別帳號？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.2.2.2	重要核心營運系統使用者除採一般使用者識別帳號外，是否考量採用適切的替代身份鑑別技術？例如：動態密碼、智慧卡或生物量測方法等。		◎	□ 適用 □ 不適用 說明：	
2.2.2.3	是否有通行碼保護措施？			□ 適用 □ 不適用 說明：	□ 以加密的方式儲存和傳送使用者通行碼
2.2.2.4	在任何情形下提供使用者通行碼之前，是否進行身份確認程序？			□ 適用 □ 不適用 說明：	□ 核對識別證或其餘身份識別 □ 寄至使用者公司郵件信箱或任何電子身份確認方式
2.2.2.5	是否強制要求使用者遵守通行碼使用規範？			□ 適用 □ 不適用 說明：	□ 強制要求使用者初次登入電腦或系統後，必須立即更改預設之通行碼 □ 一定期限內未登入，則預設通行碼將失效，必須重新再申請建立 □ 定期或依規定期限(或使用次數限制)，要求變更使用者通行碼，並避免重複或循環使用舊有相同之使用者通行碼
2.2.2.6	是否強制使用者設定足夠強度之通行碼？			□ 適用 □ 不適用 說明：	□ 通行碼長度規定須超過6個字元(建議8位或以上) □ 通行碼規定需以大小寫字母及數字(或包含特殊符號)組成 □ 規定避免使用與個人有關資訊(如生日、身份證字號、單位簡稱、電話號

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					碼等)當做使用者通行密碼
2.2.2.7	是否不允許在登入過程中自動登載使用者通行碼？			□ 適用 □ 不適用 說明：	
2.2.2.8	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？			□ 適用 □ 不適用 說明：	
2.2.2.9	是否避免保留使用者通行碼的紀錄(例如：紙張、軟體檔案或手持裝置)， 除非其能被安全地存放，且該存放方式經過核准？		◎	□ 適用 □ 不適用 說明：	
2.2.2.10	是否要求使用者於聘僱條款與條件中，簽署保密的聲明？		◎	□ 適用 □ 不適用 說明：	
2.2.2.11	對於核心營運系統異常登入程序，是否留有紀錄，並由專人定期檢視？		◎	□ 適用 □ 不適用 說明：	
2.2.2.12	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)？			□ 適用 □ 不適用 說明：	
2.2.2.13	針對連續登入錯誤的鎖定，是否訂定解鎖驗證或重新取得授權的程序？		◎	□ 適用 □ 不適用 說明：	
2.2.2.14	是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資訊？		◎	□ 適用 □ 不適用 說明：	
2.2.3 含有客戶個人資料之紙本與可移除式媒體不可置放於桌面，電腦並應設定螢幕保護程式予以鎖定。					
2.2.3.1	敏感之紙本、USB 隨身碟、隨身硬碟，是否未置於不受保護之桌面上？			□ 適用 □ 不適用 說明：	
2.2.3.2	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？			□ 適用 □ 不適用 說明：	□ 無人使用之電腦已關機或登出 □ 電腦已設定 15 分鐘以內啟動之螢幕保

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					護程式
2.2.3.3	是否訂有敏感或重要的營運資訊之桌面淨空與螢幕淨空規定？		◎	□ 適用 □ 不適用 說明：	
2.2.4 核心營運系統所在之網路應進行網路區隔，並針對連線進行限制。					
2.2.4.1	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)？			□ 適用 □ 不適用 說明：	□ 區隔內外部網路 □ 建立 DMZ 區 □ 存取敏感資料之網路予以隔離
2.2.4.2	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？			□ 適用 □ 不適用 說明：	□ 備有防火牆區隔網路
2.2.4.3	是否針對電子郵件、單雙向檔案傳輸作必要之安全控制措施？			□ 適用 □ 不適用 說明：	□ 限制電子郵件傳檔 □ 限制對外即時通訊檔案傳輸
2.2.4.4	是否設有檢測連線的來源位址與目的位址網路路由之控管措施？		◎	□ 適用 □ 不適用 說明：	
2.2.4.5	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？			□ 適用 □ 不適用 說明：	
2.2.4.6	核心營運系統使用者(含外單位人員)是否取得正式存取授權？		◎	□ 適用 □ 不適用 說明：	
2.2.4.7	是否自動識別已授權允許存取核心營運系統(包含僅存取部分敏感或機密資訊)之特定設備或來自特定地點的連線，其餘設備及連線之存取行為予以禁止？		◎	□ 適用 □ 不適用 說明：	□ 允許連線之來源或特定設備清單 □ 限制未允許連線之來源或設備之控管措施
2.2.4.8	核心營運系統的遠距工作是否得到管理階層授權(如執行政策、計畫及流程等)和施以必要之保護措施(執行前開放授權、結束後存取權限撤銷或停用、強制設備歸還等)與鑑別機制。		◎	□ 適用 □ 不適用 說明：	
2.2.5 核心營運系統之公用程式應用(如遠端連線程式、外部連線存取等)應進行管制。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.2.5.1	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)？			□ 適用 □ 不適用 說明：	□ 限制遠端連線 □ 限制 telnet 連線 □ 限制 FTP 連線
2.2.6 核心營運系統之連線時間應進行管制。					
2.2.6.1	對於核心營運系統，是否限制網路會談結束或超過界定的未動作時限後，即予中斷連線或關閉設備？			□ 適用 □ 不適用 說明：	
2.2.6.2	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？			□ 適用 □ 不適用 說明：	
2.2.6.3	對風險高的核心營運系統(如需處理機敏性資料或個人資料之業務)是否依照作業別之存取權限管制需求設定連線時間限制？		◎	□ 適用 □ 不適用 說明：	□ 連線時間限制在正常辦公時間內 □ 連線時間限制在作業需求時間
2.3 核心營運系統機房與作業環境實體安全					
2.3.1 應確保重要資料處理及辦公區域之實體安全，避免竊盜或損害。					
2.3.1.1	是否適當的使用牆、刷卡門禁控制或人員駐守的接待櫃檯等屏障，保護重要資料處理及辦公區域之安全並確保只有經授權人員方可允許進出？			□ 適用 □ 不適用 說明：	□ 門禁管制 □ 防護或隔離措施
2.3.1.2	實體邊界發生異常狀況時，是否有權責人員可立即解決？		◎	□ 適用 □ 不適用 說明：	
2.3.1.3	具有關鍵或敏感的重要資料處理及辦公區域，是否對於授權進出人員作必要之限制與監督其活動？		◎	□ 適用 □ 不適用 說明：	□ 門禁管制或登記 □ 備有監視錄影設備 □ 備有監視錄影設備 □ 定期審查、更新，並於必要時廢止進出權限設定
2.3.1.4	重要入口與內部作業環境是否備有監視錄影設施，並維持一定時間以上之紀錄？			□ 適用 □ 不適用 說明：	□ 備有監視錄影設備 □ 存有一週以上之錄影紀錄
2.3.1.5	是否備有適當的實體入侵偵測系統？		◎	□ 適用 □ 不適用 說明：	□ 備有保全設施或警鈴

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.3.1.6	是否設計並施行適當的控制措施以保護顯示敏感重要資料處理及辦公區域地點的通訊錄和內部人員名單與聯繫方式？		◎	□ 適用 □ 不適用 說明：	
2.3.1.7	是否針對訪客的拜訪紀錄(訪客進入及離開時間、訪客身份等)進行適當保護？		◎	□ 適用 □ 不適用 說明：	
2.3.1.8	接待人員或警衛是否檢查訪客是否帶走未經授權的物品？			□ 適用 □ 不適用 說明：	
2.3.1.9	重要資料處理及辦公區域是否能執行必要的滅火防護措施？			□ 適用 □ 不適用 說明：	□ 裝設自動火災警報系統或設置滅火設備 □ 作業人員熟悉自動滅火系統運作，或滅火器位置與操作方法
2.3.1.10	是否設計並施行適當之控制措施，以監督重要資料處理及辦公區域內之工作，並確保其需知原則？		◎	□ 適用 □ 不適用 說明：	
2.3.2 應確保核心營運系統機房之實體安全，避免機房遭遇破壞或損害。					
2.3.2.1	核心營運系統機房是否至少遵循重要資料處理及辦公區域之實體安全規範，以確保機房實體安全？			□ 適用 □ 不適用 說明：	
2.3.2.2	網路平台商管理的核心營運系統資訊處理設施(如：通訊服務設施)在實體上是否與第三方管理(如：客戶代管設備)的資訊處理設施區隔？		◎	□ 適用 □ 不適用 說明：	
2.3.2.3	核心營運系統電腦機房內是否嚴禁使用未經核准之電器或其他物品？			□ 適用 □ 不適用 說明：	
2.3.2.4	核心營運系統電腦作業區(含機房)是否落實執行失火防災規定？			□ 適用 □ 不適用 說明：	□ 機房與易燃物或危險物料保持安全距離 □ 嚴禁抽菸及飲食 □ 無易燃雜物或紙箱堆積

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.3.2.5	在核心營運系統之安全區域內，是否未經授權，不允許使用拍照、錄影、錄音和其他記錄性設備(如：行動裝置上的照相機)？		◎	☐ 適用 ☐ 不適用 說明：	
2.3.2.6	重要核心營運系統資訊設備之設置地點(如：核心營運系統機房)是否盡可能檢查及評估鄰近場所的任何安全威脅(如火災、風災、土石流、灰塵、水災、震動、化學效應、電力供應、電磁幅射、儲存危險物場所、民間暴動及其他天然或人為災難等可能對設備之危害)，並據以選擇適當地點？		◎	☐ 適用 ☐ 不適用 說明：	☐ 機房為抗震建物 ☐ 機房樓層地板有足夠的承載能 ☐ 統機房使用(或重要部分使用)防火建材 ☐ 統機房之設計可能降低或避免火災蔓延
2.3.2.7	核心營運系統的備援設備與備份媒體存放位置，是否與主要場地保持安全距離？		◎	☐ 適用 ☐ 不適用 說明：	
2.3.2.8	重要核心營運系統資訊處理設施是否與一般收發、裝卸區及其他未經授權人員可進入之作業場所作適當之進出區隔控制措施？		◎	☐ 適用 ☐ 不適用 說明：	
2.3.2.9	核心營運系統資訊處理相關設施是否置放於機櫃或桌上？			☐ 適用 ☐ 不適用 說明：	
2.3.2.10	是否備有空調設備並監控溫度與濕度？			☐ 適用 ☐ 不適用 說明：	☐ 有空調設備 ☐ 有溫濕度監測紀錄 ☐ 有溫濕度監控設備 ☐ 有溫濕度監控及調節設備
2.3.2.11	核心營運系統關鍵設施是否備有UPS 不斷電系統？			☐ 適用 ☐ 不適用 說明：	
2.3.2.12	核心營運系統關鍵設施是否有接地設施、以及足夠電力保護(如：雙Power 設計、定期檢測備援電源等)？		◎	☐ 適用 ☐ 不適用 說明：	
2.3.2.13	是否具備環控設備，以自動機制掌握核心營運系統資訊處理設施之環境狀況？		◎	☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.3.2.14	核心營運系統機房是否採用高架地板？並應考量重量承載能力、耐震功能，並部署地網。		◎	□ 適用 □ 不適用 說明：	
2.3.2.15	電信纜線(telecommunications lines)、網路佈纜(network cabling)及電源纜線是否置於塑膠管線保護或適當的隔離方式以防止互相干擾？		◎	□ 適用 □ 不適用 說明：	
2.3.2.16	核心營運機房各項設備是否依據供應者建議的保養間隔與規格來維護並定期檢查，以確保其可用性及完整性？		◎	□ 適用 □ 不適用 說明：	
2.3.2.17	設備之維護與修理是否僅由授權之維護人員執行？			□ 適用 □ 不適用 說明：	
2.3.2.18	是否保存所有可疑或實際的系統錯誤及所有預防性、矯正性的維護紀錄？		◎	□ 適用 □ 不適用 說明：	
2.3.3 核心營運系統機房與辦公區域外之設備應設計安全措施，保護場所管控外設備之安全。					
2.3.3.1	無人看管之核心營運系統相關設施(如：Hub、Switch)是否上鎖並定期檢查？			□ 適用 □ 不適用 說明：	□ 予以上鎖 □ 定期檢查
2.3.3.2	行動裝置(設備)是否訂有嚴謹的保護措施(如使用授權管理、設通行碼、檔案加密、專人看管)？		◎	□ 適用 □ 不適用 說明：	
2.3.4 設備外送或淘汰前應進行安全措施，防止資訊外洩。					
2.3.4.1	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？			□ 適用 □ 不適用 說明：	□ 移除版權軟體 □ 進行格式化
2.3.4.2	含有敏感性資訊的設備汰除後，是否根據風險評鑑決定是否以實體銷毀？		◎	□ 適用 □ 不適用 說明：	
2.3.4.3	攜出安全場所外之設備和媒體(如隨身碟、光碟片)是否訂有安全保護措施？		◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.3.4.4	是否明確制定核心營運系統資訊設備(包括場外使用的設備，以及財產攜出入)之控制措施，以降低對資料未經授權存取的風險、遺失及損害？		◎	☐ 適用 ☐ 不適用 說明：	☐ 攜出安全場所外使用，均經事前授權，並於攜出場外與歸還時進行安全查核且記錄
2.3.4.5	設備送安全場所外維修時，是否刪除儲存在設備內之客戶個資與交易資訊？或指派專人在場確保個資不外洩？			☐ 適用 ☐ 不適用 說明：	☐ 刪除客戶資料 ☐ 進行格式化 ☐ 指派專人監督作業
2.4 核心營運系統資料庫安全管理					
2.4.1 核心營運系統的資料庫應建立連線管制與存取控制機制，以保護消費者資料與交易資訊。					
2.4.1.1	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。			☐ 適用 ☐ 不適用 說明：	
2.4.1.2	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？			☐ 適用 ☐ 不適用 說明：	
2.4.1.3	應用軟體開發者進行連結與資料存取時是否限制只能使用無法異動資料庫的相關檔案或無作業系統權限的應用程式連結帳號？		◎	☐ 適用 ☐ 不適用 說明：	☐ 應用軟體開發者無資料庫系統或資料庫主機作業系統帳號 ☐ 應用軟體開發者使用之應用程式連結帳號無資料庫檔案異動權限及作業系統操作權限 ☐ 應用軟體開發者使用之應用程式連結帳號有存取監控紀錄
2.4.1.4	是否評估範例程式與範例資料庫的安全性，並移除不必要之範例資料？			☐ 適用 ☐ 不適用 說明：	
2.4.1.5	每個存有客戶資料之營運系統，存放於同一個資料庫管理系統(DBMS)時，是否以單一獨立資料庫為原則，禁止合併共用單一資料		◎	☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	庫？				
2.4.1.6	應用系統資料本身之安全性不同，是否由應用程式開發者使用加解密功能對資料庫內資料進行存取，避免資料庫管理者可直接解讀機密資料?		◎	□ 適用 □ 不適用 說明：	
2.4.1.7	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？			□ 適用 □ 不適用 說明：	
2.4.1.8	資料庫驗證除有特殊需求，是否禁止將帳號的通行密碼寫於不需組譯之應用程式原始碼或 Script 中？			□ 適用 □ 不適用 說明：	
2.4.2 核心營運系統的資料庫應定期查檢，以保護消費者資料與交易資訊之正確與完整。					
2.4.2.1	資料庫專任管理人員是否每日完成資料庫日常檢核作業表單或紀錄？			□ 適用 □ 不適用 說明：	
2.4.2.2	資料庫專任管理人員所屬權責主管，是否每月不定期抽驗資料庫日常檢核作業表單 N(N>=1)次以上並簽核存檔，確保紀錄確實性？			□ 適用 □ 不適用 說明：	
2.4.2.3	資料庫日常檢核作業表單是否至少但不限於包含以下項目？(1) Database Information (2) Database Archive/Transaction Log Directory Utilization (3) DB Space and Utilization (4) Check Backup Log (5)Check Database Log (6) Check Session Amount。			□ 適用 □ 不適用 說明：	
2.4.2.4	是否有資料庫遭遇重大問題事件且會影響系統服務之障礙處理流程？		◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.4.2.5	是否建立包含但不限於以下之資料庫監控預警項目？ (1)資料庫空間使用超過 N%(依據營運特性所訂之特定臨界數值)，發送簡訊通知資料庫管理人員處理。 (2)資料庫剩餘的空間不足 N 天的使用量，發送 E-Mail 通知資料庫管理人員處理。 (3)每隔 N 分鐘(依據營運特性所訂之特定臨界數值)會與資料庫做連結測試，當無法正常連結到資料庫時即發出警訊，發送簡訊與 E-Mail 通知資料庫管理人員處理。 (4)依資料庫與營運特性訂出監控使用者連線數量之臨界值，當超過臨界值時發送簡訊與 E-Mail 通知資料庫管理人員處理。 (5)當使用者的帳號未更改密碼即將超過規範之 N 天之前，從第 N-10 天開始即每天發送 E-Mail 通知帳號的所有者。		◎	□ 適用 □ 不適用 說明：	□ 監控資料庫空間使用超過 N% □ 監控資料庫資料庫剩餘的空間不足 N 天的使用量 □ 監控資料庫連結 □ 監控使用者連線數量之臨界值 □ 自動過濾使用者的帳號未更改密碼即將超過規範之 N 天的名單
2.4.2.6	是否驗證存取任何資料庫的所有操作？包括應用程式、管理員和所有其他使用者的存取操作。		◎	□ 適用 □ 不適用 說明：	
2.4.3 核心營運系統之資料庫應定期備份。					
2.4.3.1	核心營運系統是否依照備份政策定期執行並依照「電子商務交易安全規範-網路平台 4.1.4」各項查檢項目，留存作業查檢紀錄？			□ 適用 □ 不適用 說明：	
2.4.4 核心營運系統之資料庫應留存重要存取紀錄。					
2.4.4.1	資料庫管理者之操作行為是否記錄？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.4.4.2	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。			□ 適用 □ 不適用 說明：	
2.5 核心營運系統營運持續安全管理					
2.5.1 電子商務核心流程應訂定能確保及時復原必要運作之營運持續計畫。					
2.5.1.1	是否發展與實作電子商務核心流程之營運持續計畫，以確保能及時復原必要的運作？			□ 適用 □ 不適用 說明：	□ 備有營運持續計畫
2.5.1.2	是否針對所有的電子商務核心營運流程，對可能造成營運中斷之機率及衝擊進行風險評鑑？(包含產業供應鏈上下游業者，如關鍵網路、電信設備及資訊設施委外管理服務、維運或設備維護等)		◎	□ 適用 □ 不適用 說明：	
2.5.1.3	是否擬定營運中斷後各風險之處理優先順序或處理準則？		◎	□ 適用 □ 不適用 說明：	□ 包含處理順序說明 □ 最低營運水準定義 □ 處理方式或準則
2.5.1.4	是否識別關鍵電子商務核心流程及排定優先順序？		◎	□ 適用 □ 不適用 說明：	
2.5.1.5	是否依據流程優先與風險鑑別擬訂之營運持續計畫(含啟動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、 所須資源、往來單位之應變規劃、合約適當性及產業供應鏈上下游業者資源等)？			□ 適用 □ 不適用 說明：	□ 備有各種情境之營運持續計畫
2.5.1.6	是否訂各項營運持續分項計畫之緊急應變處理程序？並定期演練及測試？分項計畫包含但不僅線如下： (1)依據維運場地與機房所處縣市與實際環境，訂定諸如水災、風災、地震、停電、土石流、傳染病		◎	□ 適用 □ 不適用 說明：	□ 備有營運持續計畫之分項計畫 □ 備有與維運場所遭遇天然災害之營運持續計畫之緊急應變處理程序與災害復原作業程序

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	等台灣常見嚴重災害發生時，電子商務平台營運持續計畫與災害復原處理作業程序？ (2)遭惡意程式攻擊後復原的營運持續計畫，並包括所有必要的資料與軟體備份及復原安排？				☐ 備有遭惡意程式攻擊後復原的營運持續計畫，並包括所有必要的資料與軟體備份及復原安排 ☐ 有定期演練測試紀錄
2.5.1.7	營運持續計畫是否以人員安全為優先，並保護資訊處理設施和公司財產？		◎	☐ 適用 ☐ 不適用 說明：	
2.5.1.8	是否考量設立異地機房與異地辦公場所，以備核心營運系統可於重大災害發生後於短期內恢復營運？		◎	☐ 適用 ☐ 不適用 說明：	
2.5.1.9	營運持續計畫是否定期完整測試、演練並更新維護?			☐ 適用 ☐ 不適用 說明：	☐ 定期進行紙本推演 ☐ 定期進行實際演練 ☐ 定期依需求更新計畫內容
2.5.1.10	營運持續計畫(含緊急應變處理程序)是否配合業務、公司、產業供應鏈上下游及人員之變更而更新？		◎	☐ 適用 ☐ 不適用 說明：	
3. 強化客戶個人資料安全管理					
3.1 客戶資料隱私管理					
3.1.1 應於網站或公司營運據點所屬範圍之適當地點公告隱私權保護宣告或政策，相關資訊至少包含客戶資料蒐集與利用範圍、第三方協同作業範圍、資料保護安全措施等。					
3.1.1.1	是否於網站或公司營運據點所屬範圍之適當地點，公告隱私權保護宣告或政策？			☐ 適用 ☐ 不適用 說明：	☐ 客戶資料蒐集與利用範圍 ☐ 第三方協同作業範圍 ☐ 資料保護安全措施
3.1.2 應成立管理組織並依作業需求指定作業人員之權責，以依相關法令辦理安全維護及客戶個人資料保管事項。					
3.1.2.1	處理或保有客戶個人資料之部門，是否指定作業專責人員依相關法令辦理安全維護及客戶個人資料保管事項？			☐ 適用 ☐ 不適用 說明：	
3.1.3 應設置並對外公告「客戶個人資料保護聯絡窗口」，協調聯繫客戶資料事宜，及擔任消費者提出申訴與救濟時之單一窗口。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.1.3.1	是否設置「客戶個人資料保護聯絡窗口」，協調聯繫客戶資料事宜，並將聯繫方式(如：電話、E-mail)置於公司網站，以便利消費者提出申訴與救濟？			□ 適用 □ 不適用 說明：	
3.1.4 應辨識電子商務營運流程中，「客戶個人資料保護」可能遭遇的重大風險(如駭客入侵竊取個資等)，建立並執行具體因應對策。					
3.1.4.1	是否瞭解、定義與記錄保有客戶個人資料之相關風險？			□ 適用 □ 不適用 說明：	
3.1.4.2	是否進行特定客戶個人資料種類(如法令規定限制蒐集等)之風險評估？		◎	□ 適用 □ 不適用 說明：	
3.1.4.3	是否進行特定客戶個人資料種類之風險建立控管措施(如符合法令規定應進行管控之特定來源)？		◎	□ 適用 □ 不適用 說明：	
3.2 客戶資料盤點作業					
3.2.1 應定期盤點電子商務營運服務流程(包含輸入與輸出)所涉及的客戶個人資料之敏感等級、儲存使用方式、傳輸媒介、接觸人員等，並評估其相對應的安全維護措施之強度。					
3.2.1.1	是否瞭解、定義與記錄保有客戶個人資料之種類與數量？			□ 適用 □ 不適用 說明：	
3.2.1.2	是否區分客戶資料種類之等級？			□ 適用 □ 不適用 說明：	
3.2.1.3	是否識別客戶資料種類之儲存使用方式？			□ 適用 □ 不適用 說明：	
3.2.1.4	是否識別客戶資料種類之傳輸方式？			□ 適用 □ 不適用 說明：	
3.2.1.5	是否識別客戶資料於電子商務流程中之接觸人員？			□ 適用 □ 不適用 說明：	
3.2.1.6	是否鑑別客戶資料於電子商務流程中現有之安全措施強度？			□ 適用 □ 不適用 說明：	
3.3 客戶資料依法對外公開、資訊揭露作業					
3.3.1 應依據法律規定、契約及正式對外宣告之隱私權政策，並於蒐集時即告知客戶相關					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
訊息，始得執行客戶個人資料對外公開、資訊揭露等作業。					
3.3.1.1	若必須公開或揭露客戶個人資料給第三方單位，公司是否已檢查揭露客戶個人資料給第三方之作業依據法令並取得客戶同意？			☐ 適用 ☐ 不適用 說明：	
3.3.1.2	若客戶個人資料需公開或揭露給第三方單位，是否確保第三方可提出其存取個人資料之權利或法令依據？並於必要時提出其第三方身分識別資料？			☐ 適用 ☐ 不適用 說明：	
3.3.1.3	若必須公開或揭露客戶個人資料給第三方單位，是否經過檢查手續，確保僅揭露最少數量之客戶個人資料項目給第三方？			☐ 適用 ☐ 不適用 說明：	
3.3.1.4	若必須公開或揭露客戶個人資料給第三方單位，是否留存相關作業紀錄並確保可查詢到客戶同意或法令之依據？			☐ 適用 ☐ 不適用 說明：	
3.3.1.5	若需於公司管理之網站或網頁公布個人資料時，是否經所屬部門主管核准，並依相關法律及規範處理？			☐ 適用 ☐ 不適用 說明：	
3.3.2 所訂定之「客戶個人資料保護政策與程序」應包含所有線上及離線作業，明確規定客戶資料對外公開、資訊揭露作業之期間、地區、對象、處理方式與保護範圍(界定交易網頁由平台業者或委外第三方單位控管)。					
3.3.2.1	是否訂定客戶個人資料保護之程序與政策？		◎	☐ 適用 ☐ 不適用 說明：	☐ 包含規範客戶資料對外公開、資訊揭露作業之期間、地區、對象、處理方式與保護範圍(界定交易網頁由平台業者或委外第三方單位控管)
3.4 客戶資料蒐集、處理及儲存管理作業					
3.4.1 蒐集、處理或利用客戶個人資料時，應依照法令規定，透過文字描述其合理關連之特定目的、使用方式及消費者個人資料相關權利之行使方式，並取得當事人同意。					
3.4.1.1	蒐集、處理或利用客戶個人資料時，是否透過文字描述其合理關連之特定目的，並經當事人書面同意？			☐ 適用 ☐ 不適用 說明：	☐ 說明特定目的 ☐ 取得書面同意 ☐ 不符合

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.4.1.2	是否未有法律、合約依據而蒐集、處理或利用下列客戶個人資料項目：醫療、基因、性生活、健康檢查及犯罪前科之相關個人資料？			□ 適用 □ 不適用 說明：	
3.4.1.3	向當事人蒐集客戶個人資料時，是否明確告知消費者蒐集個人資料之目的、類別、利用期間、地區、揭露對象及方式？			□ 適用 □ 不適用 說明：	
3.4.1.4	向消費者蒐集個人資料時，是否明確告知其以下得行使之權利及方式？(1)查詢或請求閱覽。(2)請求製給複製本。(3)請求補充或更正。(4)請求停止蒐集、處理或利用。(5)請求刪除。			□ 適用 □ 不適用 說明：	
3.4.1.5	是否依消費者請求，就其蒐集之個人資料，提供答覆查詢、閱覽、製給複製本之權利與程序，並於 10 日內予以回應及留存申請紀錄？			□ 適用 □ 不適用 說明：	
3.4.1.6	蒐集非由消費者當事人提供之個人資料，是否於處理或利用前，向其告知個人資料來源、目的、類別、利用期間、地區、揭露對象及方式？			□ 適用 □ 不適用 說明：	
3.4.2 應對保有客戶個人資料之部門員工宣導與規範禁止向任何未經授權的第三人交付、揭露、出售或轉讓所蒐集之個人資料，並認知其保護個資之職責。					
3.4.2.1	是否對保有客戶個人資料之部門員工宣導與規範禁止向任何第三人交付、揭露、出售或轉讓所蒐集之個人資料，並認知其保護個資之職責？			□ 適用 □ 不適用 說明：	
3.4.2.2	是否對處理客戶個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練，並定期於部門內宣導個資隱私保護之重要性？			□ 適用 □ 不適用 說明：	
3.4.3 應於向三方揭露或由委外廠商處理客戶個人資料前，確保其合法性並取得對客戶個人資料安全保護之能力與承諾。					
3.4.3.1	是否確保向第三方揭露或由委外廠商處理客戶個人資料時，確保其合法性與資料安全？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.4.3.2	是否要求受委託處理客戶個人資料之外部團體或個人，簽署個人資料之保密切結書？			□ 適用 □ 不適用 說明：	
3.4.4 客戶個人資料之處理行為應經權責單位核准，並訂定個人資料管理之稽核程序及設置稽核人員以定期審查作業情形並留存相關稽核紀錄。					
3.4.4.1	客戶個人資料之處理行為是否經權責單位核准？			□ 適用 □ 不適用 說明：	
3.4.4.2	處理客戶個人資料檔案之人員是否有授權核准及異動管理？			□ 適用 □ 不適用 說明：	□ 作業人員簽訂與客戶隱私保護相關條款之保密切結書 □ 離職時，規定應取消或停用其使用者識別帳號並收繳通行證件 □ 職務異動時，規定應列冊移交相關媒體及資料 □ 職務異動時，接替人員應於相關系統重設帳號密碼，並視需要更換使用者帳號
3.4.4.3	客戶個人資料之輸出入與處理個人資料檔案之個人電腦，是否均以帳號密碼管制？			□ 適用 □ 不適用 說明：	□ 必須以帳號密碼登入 □ 該帳號不與其他人員或作業共用
3.4.4.4	客戶個人資料之處理行為是否留存使用者身分與其行為紀錄以供事後稽查？			□ 適用 □ 不適用 說明：	□ 留存使用者身份登出入紀錄 □ 留存存取客戶資料紀錄
3.4.4.5	客戶個人資料檔案之更新、更正或註銷是否均報經核准？			□ 適用 □ 不適用 說明：	
3.4.4.6	客戶個人資料檔案之更新、更正、註銷內容、作業人員及時間是否詳實記錄？			□ 適用 □ 不適用 說明：	
3.4.4.7	是否經單位主管授權執行個人資料管理之稽核作業，並存有稽核紀錄？			□ 適用 □ 不適用 說明：	□ 留有稽核紀錄

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.4.4.8	經內、外部稽核人員提出之建議事項，是否有後續之矯正及預防措施？			□ 適用 □ 不適用 說明：	□ 留有後續改善紀錄
3.4.4.9	各運用客戶資料之系統平台、資料庫及應用程式是否開啟日誌功能，或至少儲存資料庫之存取紀錄6個月，以供日後稽核使用？		◎	□ 適用 □ 不適用 說明：	
3.4.5 存放客戶個人資料檔案(含數位與紙本檔案)之主機、週邊設備及相關設施等，應置於內部至少第二層門禁管制之安全作業區域(或上鎖檔案櫃)，建立完整管理監督程序並留存相關紀錄。					
3.4.5.1	對存放客戶個人資料檔案之主機、週邊設備及相關設施等，是否置放於實體安全區域？			□ 適用 □ 不適用 說明：	□ 置於門禁控管之辦公區域、機房
3.4.5.2	儲存客戶個人資料檔案之場所，是否建立門禁管制並落實執行？			□ 適用 □ 不適用 說明：	□ 備有進出登記 □ 備有門禁紀錄
3.4.5.3	儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，是否指定專人管理並有獨立存放空間(如：鐵櫃)與上鎖保管？			□ 適用 □ 不適用 說明：	□ 指定專人保管 □ 置於上鎖之鐵櫃
3.4.5.4	儲存個人資料檔案之媒體(如磁片、光碟片及磁帶)是否有攜出、拷貝或複製的管控機制，並留存紀錄？			□ 適用 □ 不適用 說明：	
3.4.5.5	客戶個人資料存放之機房或庫房，是否備有監視錄影監控並留存紀錄？			□ 適用 □ 不適用 說明：	□ 備有監視錄影設施 □ 留存一週以上之影像紀錄
3.4.5.6	是否將存放客戶個人檔案資料的電腦與外部網路之連線執行隔離管制？			□ 適用 □ 不適用 說明：	□ 建置防火牆與外部網路隔絕
3.4.5.7	存放個人資料之資訊設備是有落實基本安全防護？			□ 適用 □ 不適用 說明：	□ 安裝防毒軟體並每日更新病毒碼 □ 每週執行完整掃描 □ 定期更新作業系統漏洞 □ 定期更新應用程式漏洞
3.4.5.8	筆記型公務電腦內是否未儲存客戶個人資料？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.4.5.9	是否未將客戶個人資料儲存於任何可攜式(Portable)儲存媒體中，如USB 隨身碟？			□ 適用 □ 不適用 說明：	
3.4.5.10	儲存客戶個人資料檔案之媒體與資料，是否建立備份或備援機制？			□ 適用 □ 不適用 說明：	□ 建置備援設備 □ 留有備份 □ 更新設備時，進行客戶個人資料備份後執行安全的移除
3.4.5.11	與客戶個人資料有關之電腦設備，是否由資料保管單位進行客戶資料之回復測試計畫或程序？		◎	□ 適用 □ 不適用 說明：	□ 訂定客戶資料回覆計畫 □ 測試資料回復
3.5 客戶資料使用及傳輸安全作業					
3.5.1 客戶個人資料之使用、傳遞與交換作業等相關資訊，應於蒐集當時、變更時告知並取得當事人同意。					
3.5.1.1	利用客戶個人資料行銷時，是否經當事人書面同意？			□ 適用 □ 不適用 說明：	
3.5.1.2	客戶相關個人資料不得提供非該次交易必要範圍外之使用；如需變更資料利用之目的，是否重新以書面取得當事人之同意？			□ 適用 □ 不適用 說明：	
3.5.2 需以企業網路與外部廠商或客戶交換之資料，應有適當加密或其他保全機制，不得明碼傳送。					
3.5.2.1	如需傳遞或複製機密資料給予公司外部之第三者時，是否確認此外部第三者已與公司簽訂載明雙方權利義務之保密協議書或相關且有法律效力之安全文件？			□ 適用 □ 不適用 說明：	□ 訂定保密協議
3.5.2.2	與外部廠商或人員交換電子客戶個人資料時，是否採取可靠且具備保密機制之傳遞方式？			□ 適用 □ 不適用 說明：	□ 檔案加密 □ 透過專屬安全連線與帳號、通行密碼
3.5.3 客戶個人資料之使用、傳遞與交換作業(包含國際傳輸)，應有安全的作業機制，明確規定執行作業之期間、地區、對象、申請及處理方式，並留存定期查檢紀錄。					
3.5.3.1	因業務需求，欲遞送、交換紙本客戶個人資料給予內部其他負責單位時及紙本資料回收時，是否將客戶個人資料裝入專用信封後並加以密封？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.5.3.2	因業務需求交換電子客戶個人資料給予公司內部其他單位負責人員處理時，是否將檔案加密？			□ 適用 □ 不適用 說明：	
3.5.3.3	以紙本或電子行式交換個人資料時，是否記錄轉交或傳輸行為之流向？			□ 適用 □ 不適用 說明：	
3.5.3.4	對於個人資料之調閱，是否有申請及核准程序？申請表單內容至少須包括但不限於「調閱者」、「申請目的」、「使用週期」、「預計使用期限」、「資料欄位需求」等項目。			□ 適用 □ 不適用 說明：	
3.5.3.5	客戶個人資料保管單位完成申請需求後，使用單位是否依規定之個人資料保護、保管、傳遞等規範進行資料之使用？		◎	□ 適用 □ 不適用 說明：	
3.5.3.6	任何含有客戶資料的文件或電子媒體(如隨身碟、磁片、光碟片及磁帶)，其複製行為是否在規劃的伺服器或安全磁碟區中執行？		◎	□ 適用 □ 不適用 說明：	
3.5.3.7	含有客戶資料之查詢存取及相關系統登入，是否使用雙重識別認證(如：生日+身分證字號或行動電話號碼+取件地點，或帳號密碼+動態密碼或簡訊或隨機碼驗證或電子郵件驗證)的方式為之？			□ 適用 □ 不適用 說明：	
3.5.3.8	部門因工作職務需求，需列印相關客戶資料之文件或報表，且該資料(如報表、公文)需以保存/歸檔一定期限以上者，是否由各部門建立「資料檢查清單」予以控管？		◎	□ 適用 □ 不適用 說明：	
3.5.3.9	是否針對客戶個人資料檔案之列印進行管制與紀錄？			□ 適用 □ 不適用 說明：	□ 限制作業上無列印需求的員工之列印功能控管 □ 取消非正職人員印製報表之權限 □ 只開放正職人員或有業務需求者有列印權限 □ 客戶個人資料檔案

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					之列印授權皆有紀錄
3.5.3.10	針對客戶個人資料相關系統規劃及設計之協力廠商，是否由系統負責部門控管該協力廠商之閱讀及印製權限，並查核系統使用紀錄？			□ 符合 □ 不符合	
3.5.3.11	客戶個資處理作業相關人員於作業中離開座位或下班，是否將電腦予以鎖定或關機，避免相關電子型式的客戶個人資料暴露於外？			□ 符合 □ 不符合	□ 電腦設定以通行密碼保護之螢幕保護程式 □ 鎖定電腦
3.5.3.12	客戶個人資料檔案使用完畢後，是否立即退出應用程式？			□ 符合 □ 不符合	
3.5.3.13	是否禁止透過端點作業散佈個客戶個人資料之行為？			□ 符合 □ 不符合	□ 禁止開啟網路芳鄰分享客戶個人資料目錄與檔案 □ 限制 MSN 傳輸檔案 □ 限制 P2P 傳輸 □ 限制使用外部網頁式電子郵件
3.5.3.14	客戶個人資料疑似被竊取、洩漏、竄改或其他侵害時，是否建立相關機制，查明後以適當方式通知當事人，並備有相關的事故管理計畫以防止事故擴大？		◎	□ 適用 □ 不適用 說明：	
3.6 客戶資料正確性維護作業					
3.6.1 應訂定有明確作業步驟與作業周期性以更新、維護客戶個人資料，於必要時應及時更新，並留下相關作業查核紀錄。					
3.6.1.1	是否制定程序，在必要時及時更新客戶個人資料？			□ 適用 □ 不適用 說明：	□ 定期提醒客戶更新資料 □ 配合客戶需求更新資料
3.6.2 應對客戶提出其個人資料諮詢、更新與申訴等服務時，有完整的執行步驟與客戶回應說明。					
3.6.2.1	是否制定關於客戶個人資料諮詢與申訴的相關處理程序？			□ 適用 □ 不適用 說明：	□ 備有客戶個資處理之標準作業程序
3.6.3 利用電腦處理客戶個人資料時，應有內部作業查驗程序，以確保輸入資料與原資料					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
相符合。					
3.6.3.1	利用電腦處理客戶個人資料時，是否有相關查驗程序確保輸入資料與原資料相符合？			□ 適用 □ 不適用 說明：	□ 備有資料輸入抽核機制
3.6.4 客戶欲維護個人資料之正確性或發生爭議時，應於 30 日內予以回應處理狀況，並尊重消費者權益與意願，若有提出停止處理或利用，且其要求符合法律、契約規定應立即執行。					
3.6.4.1	消費者欲維護個人資料之正確性時，是否有相關之程序主動或供當事人申請更正或補充，並於 30 日內予以回應？			□ 適用 □ 不適用 說明：	
3.6.4.2	客戶個人資料正確性發生爭議時，是否有相關之程序主動或供消費者申請停止處理或利用，並於 30 日內予以回應？			□ 適用 □ 不適用 說明：	
3.7 客戶資料刪除及停止利用作業					
3.7.1 含有客戶資料之儲存媒體之汰除，應使用格式化或其他實體破壞方式予以銷毀。					
3.7.1.1	儲存客戶個人資料檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其所儲存之客戶個人資料檔案？			□ 適用 □ 不適用 說明：	□ 刪除客戶資料 □ 進行格式化 □ 實體破壞儲存媒體
3.7.2 應每日檢查環境周遭是否有未妥善保管之客戶資料。					
3.7.2.1	是否每日檢查環境周遭是否有列印出的客戶資料，若有則一律銷毀？			□ 適用 □ 不適用 說明：	
3.7.2.2	客戶個資處理作業相關人員於作業中離開座位或下班時，是否妥善收存書面形式之客戶資料？			□ 適用 □ 不適用 說明：	
3.7.2.3	傳真設備是否由專人於特定時間檢查傳真進件之客戶個人資料是否已交至處理人員？若接獲非該部門之客戶個人資料，則依內部遞送方式轉予正確之處理單位或負責人員；若無法辨識處理單位者，是否予以碎紙銷毀？			□ 適用 □ 不適用 說明：	
3.7.3 欲廢棄或不再持有之客戶紙本資料，應使用碎紙機或其他實體破壞方式予以確實銷毀，或委由專業處理廠商於專人監督下銷毀。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.7.3.1	客戶個人資料蒐集之特定目的消失或期限屆滿時，是否有相關之程序主動或依當事人申請，刪除、銷毀、停止處理或利用該個人資料？			☐ 適用 ☐ 不適用 說明：	
3.7.3.2	各項客戶資個人料處理完成後，是否由各文件負責單位進行後續歸檔或銷毀作業？			☐ 適用 ☐ 不適用 說明：	
3.7.3.3	少量之書面文件資料若無特別規範需歸檔，或文件資料內有客戶資料、公司營運機密資訊，是否使用碎紙機銷毀？			☐ 適用 ☐ 不適用 說明：	
3.7.3.4	大量之機敏文件銷毀前是否統一分配裝箱並黏貼封條？			☐ 適用 ☐ 不適用 說明：	
3.7.3.5	為確保大量文件妥善統一銷毀，銷毀文件運送過程，是否指派專人協同至銷毀場，見證銷毀作業完成並予以照相或錄影？			☐ 適用 ☐ 不適用 說明：	
3.7.3.6	是否保留銷毀作業之收件紀錄及銷毀場之銷毀證明至少 N(N>=1)年存查？			☐ 適用 ☐ 不適用 說明：	
3.7.4 應控管電子客戶個人資料留存的時間，定期由專人或負責人員刪除，並由主管不定期抽檢。					
3.7.4.1	是否控管電子客戶個人資料留存的時間，定期由專人或負責人員刪除，並由主管不定期抽檢？			☐ 適用 ☐ 不適用 說明：	
3.7.4.2	各項電子形式之客戶資料報表，是否於完成處理作業後，應由各負責單位於報表保存期限到期前，進行檔案之刪除作業？			☐ 適用 ☐ 不適用 說明：	
3.7.4.3	特定系統之備份，是否定時於檔案轉換成備份存檔後，將資料於系統移除？			☐ 適用 ☐ 不適用 說明：	
4. 提升企業內資訊環境安全管理					
4.1 網路通訊與資訊作業安全管理					
4.1.1 重要資訊設備與通訊設施管理人員應熟悉操作程序，於重要設定變更異動設備時應留存相關核准與測試紀錄。					
4.1.1.1	資訊處理與通訊設施相關之各項			☐ 適用	☐ 電腦開機與關機程

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	作業程序及活動是否訂定文件並適當維護？			□ 不適用 說明：	序 □ 備份 □ 設備維護 □ 資訊的處理與處置 □ 異常情況之處理 □ 緊急聯絡資訊 □ 電腦機房與郵件處置管理
4.1.1.2	資訊處理設施與系統的變更是否有正式核准之程序，並向相關人員通報變更細節？			□ 適用 □ 不適用 說明：	□ 備有核准文件
4.1.1.3	資訊處理設施與系統的變更是否詳實記錄，並考量依變更程度重新進行風險評鑑？		◎	□ 適用 □ 不適用 說明：	
4.1.1.4	資訊處理設施與系統的變更是否備有 Rollback 程序，包括由不成功的變更和意外事件的中止和復原之程序與責任？		◎	□ 適用 □ 不適用 說明：	
4.1.2 含有客戶個資之重要作業職權應加以區隔，以降低資產遭未經授權或非意圖的修改或誤用之機會。					
4.1.2.1	對於安全要求高的資訊業務(如：牽涉客戶資料)，是否盡可能區隔其職務與責任領域？			□ 適用 □ 不適用 說明：	□ 職務分配表
4.1.2.2	核心營運系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否盡可能授權由不同的人員執行？			□ 適用 □ 不適用 說明：	
4.1.2.3	是否盡可能分隔開發、測試及運作之設施、系統、軟體？		◎	□ 適用 □ 不適用 說明：	□ 系統開發區 □ 系統測試區
4.1.3 應安裝防毒軟體，並定期更新病毒碼及執行系統掃描作業。					
4.1.3.1	是否定期對電腦系統及資料儲存媒體(如磁片、光碟片及磁帶)進行病毒與後門程式掃描？			□ 適用 □ 不適用 說明：	
4.1.3.2	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？			□ 適用 □ 不適用 說明：	□ 安裝防毒軟體 □ 每日更新 □ 每三日更新
4.1.3.3	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			□ 適用 □ 不適用	□ 復原程序 □ 通報流程

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	工通報惡意程式之攻擊，並執行復原程序？			說明：	
4.1.3.4	防毒系統管理人員，是否每月彙整防毒系統統計報表，呈核直屬主管？		◎	□ 適用 □ 不適用 說明：	
4.1.3.5	防毒系統管理人員處理重大病毒感染事件後(如：一定數量之群聚感染)，是否針對事件處理撰寫報告並研擬後續防禦措施，呈核直屬主管？		◎	□ 適用 □ 不適用 說明：	
4.1.3.6	使用者或訪客因業務需求，攜入非公司之資訊設備及可攜式媒體時，資訊設備是否於協請防毒系統管理人員安裝防毒軟體、最新修補程式後，才可與網路連接？		◎	□ 適用 □ 不適用 說明：	
4.1.3.7	防毒系統管理人員是否配合電子郵件系統與服務，建置電子郵件防毒閘道與安裝郵件伺服器防毒軟體？		◎	□ 適用 □ 不適用 說明：	
4.1.3.8	行動碼(mobile code)的安裝是否作必要之授權處理或限制使用？內嵌行動碼之中介軟體(middleware)是否考量其限制使用？		◎	□ 適用 □ 不適用 說明：	
4.1.4 重要資料及資訊系統應定期進行系統與軟體的備份與還原測試。					
4.1.4.1	重要的資訊及軟體是否定期作備份處理，並界定備份資訊的必要等級？			□ 適用 □ 不適用 說明：	
4.1.4.2	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？			□ 適用 □ 不適用 說明：	□ 存放於受控管之安全區域 □ 存放於上鎖存放區
4.1.4.3	是否對備份資料定期檢查與執行回復測試，以確保備份資訊之可用性及有效性且能夠在用以復原之運作程序分配的時間內完成？		◎	□ 適用 □ 不適用 說明：	□ 備份紀錄表 □ 測試紀錄表
4.1.4.4	重要及機敏資訊的備份程度與頻率是否反應產業供應鏈的營運要求？		◎	□ 適用 □ 不適用 說明：	
4.1.4.5	備份資訊是否儲存於遠端地點？距離是否足以避免機房與辦公主要場地發生災難時遭波及？		◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.1.4.6	備份資訊是否給予適切等級的實體與環境保護，並與機房與辦公主要場地使用的標準一致？(機房與辦公主要場地採用的控制措施可延伸至涵蓋備份作業場地)		◎	□ 適用 □ 不適用 說明：	
4.1.4.7	重要備份資料(含資料庫)是否考量維持一定數量的不同時期備份？		◎	□ 適用 □ 不適用 說明：	□ 存有備份資料 □ 備份週期_____ □ 備份留存__代以上
4.1.5 應定期檢測網路安全及連線品質，以確保網路的系統與應用程式的安全。					
4.1.5.1	有關網路安全之事項是否隨時公告？			□ 適用 □ 不適用 說明：	
4.1.5.2	是否定期檢討網路安全控管事項之執行？			□ 適用 □ 不適用 說明：	
4.1.5.3	是否定期檢測網路運作環境之安全漏洞？			□ 適用 □ 不適用 說明：	
4.1.5.4	通訊設備是否具備偵測網路壅塞並避免網路壅塞時通訊集中之機制？		◎	□ 適用 □ 不適用 說明：	
4.1.5.5	核心營運系統是否持續監控與其它通信服務互連的狀態？是否有適當的控制措施檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以檢查？		◎	□ 適用 □ 不適用 說明：	
4.1.5.6	託管之核心營運系統，是否已定義一旦發生斷線時如何處置的協議或合約？		◎	□ 適用 □ 不適用 說明：	
4.1.5.7	是否適當的保護網路設施避免遭受可能的網路攻擊？		◎	□ 適用 □ 不適用 說明：	□ 伺服器、路由器等具備經由 IP 位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬之機制 □ 透過存取控制清單限制特定協定(如：SNMP)之存取來源 IP 位置 □ 關閉非必要網路管

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					理之通訊協定
4.1.5.8	是否考量具備偵測偽造來源地址(IP spoofing)的能力？		◎	□ 適用 □ 不適用 說明：	
4.1.5.9	是否考量運用嚴格的加密控制措施及／或高強度憑證(strong authentication)的功能以防範來源造假(source impersonation)？		◎	□ 適用 □ 不適用 說明：	
4.1.5.10	是否考量訂定相關政策以對應阻斷服務(DoS)或分散式阻斷服務攻擊(DDoS)並建置適切之控管措施？		◎	□ 適用 □ 不適用 說明：	
4.1.5.11	是否訂定相關政策以對應垃圾郵件並建置適切之控管措施？			□ 適用 □ 不適用 說明：	
4.1.5.12	是否導入垃圾郵件過濾系統及連線過濾技術？並匯入黑白名單以阻攔大量的垃圾郵件？		◎	□ 適用 □ 不適用 說明：	
4.1.5.13	電子商務作業之電子郵件伺服器管理，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？			□ 適用 □ 不適用 說明：	
4.1.6 應安裝防火牆或入侵偵測系統，定期檢查防火牆和路由器的規則設定，以保護系統之安全。					
4.1.6.1	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？			□ 適用 □ 不適用 說明：	
4.1.6.2	防火牆管理員是否限制在指定 IP 與特定連接埠才能登入管理？		◎	□ 適用 □ 不適用 說明：	
4.1.6.3	是否將對外提供公開服務之主機群，建置於 DMZ 並保留連線紀錄？		◎	□ 適用 □ 不適用 說明：	
4.1.6.4	公司對外傳輸保護措施，是否於網路閘道端安裝過濾設備(如：傳輸內容含機敏資料將會被擷取下來，以提供稽核及主管確認及處理。)？		◎	□ 適用 □ 不適用 說明：	
4.1.6.5	無線網路之存取及應用，是否訂有嚴謹的鑑別、加密方式及頻率選擇		◎	□ 適用 □ 不適用	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	等控制措施？			說明：	
4.1.6.6	公司內若運用超過 50 台以上執行電子商務營運之個人電腦(含移動式電腦)，是否考量採用統一之網域管理機制，並設定適當之帳號管理與安全控制機制？		◎	□ 適用 □ 不適用 說明：	
4.1.6.7	是否訂定行動式之電腦及通信設備之管理政策(如實體保護、存取控制、使用之加密技術、備份及防毒要求)？			□ 適用 □ 不適用 說明：	□ 可攜帶式設備管理政策
4.1.6.8	是否對支援核心營運程序的系統之軟體與資料執行定期審查？(若出現任何未經核准的檔案或未經授權的增補，宜調查其原因)		◎	□ 適用 □ 不適用 說明：	
4.1.7 記錄使用者活動、異常及資訊安全事件，宜產生與保留一段議定的期間，以協助未來的調查與存取控制監視。					
4.1.7.1	是否考量實施適當之稽核存錄措施，以記錄與監視使用者與產業供應鏈資訊作業之活動、異常及資訊安全事件，同時涵蓋法規要求？		◎	□ 適用 □ 不適用 說明：	
4.1.7.2	資安事件日誌之紀錄內容是否包括使用者識別碼、登入登出之日期時間、電腦的識別資訊或其網址、事件描述及矯正措施等事項？		◎	□ 適用 □ 不適用 說明：	
4.1.7.3	是否建立適當之控制措施以監視資訊處理設施的使用，並定期審查各項作業日誌？			□ 適用 □ 不適用 說明：	
4.1.7.4	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？			□ 適用 □ 不適用 說明：	資料留存時限： □ 交易紀錄 □ 會計帳務 □ 客訴處理 □ 法令法規要求留存文件
4.1.7.5	存錄設施與日誌資訊是否規劃適當之儲存媒體容量，以避免無法記錄事件或覆蓋以往所記錄事件？		◎	□ 適用 □ 不適用 說明：	
4.1.7.6	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？			□ 適用 □ 不適用 說明：	□ 日誌審查紀錄

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.1.7.7	由使用者或系統程式所產生之錯誤，導致相關資訊處理或通信系統的問題是否加以存錄？並有明確之規則，處置所取得之錯誤紀錄？			□ 適用 □ 不適用 說明：	
4.1.8 所有交易相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。					
4.1.8.1	所有系統或監視器之日期與時間設定是否定期核對校正，以確保時間記錄正確？			□ 適用 □ 不適用 說明：	□ 校時紀錄或工具
4.1.8.2	電子商務作業之網路安全管理、網路服務監控與測試、防範惡意碼與行動碼等項目，是否考量參考「電子商務安全偵測機制控制項」，執行相關控管作為？			□ 適用 □ 不適用 說明：	
4.2 電子郵件安全管理(一般使用者)					
4.2.1 應制定電子郵件使用規則，以維護使用郵件的系統與應用程式的安全。					
4.2.1.1	傳遞包含客戶個資之重要資料之郵件，是否採用合宜之加密機制(如MS Office 安全性設定、PGP 加密或自然人憑證驗證等機制)？			□ 適用 □ 不適用 說明：	
4.2.1.2	敏感或機密性之客戶個資或交易資料，如需以電子郵件附件方式對外傳送，是否採用合宜的加密措施(如：壓縮軟體 RAR、ZIP 加上密碼等)處理後傳送？			□ 適用 □ 不適用 說明：	
4.2.1.3	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？			□ 適用 □ 不適用 說明：	
4.2.1.4	是否關閉電腦端郵件收發軟體			□ 適用 □ 不適用 說明：	□ 規範並落實限制電腦端郵件收發軟體(Outlook 或 Outlook Express)與 Webmail 的信件自動下載圖片(或其他內容)功能 □ 規範並落實關閉電腦端郵件收發軟體(如：Outlook 或 Outlook Express)郵件預覽功能 □ 規範並落實限制電

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					腦端郵件收發軟體(如：Outlook 或 Outlook Express)預設使用純文字模式開啟郵件
4.2.1.5	使用者是否了解電子郵件社交工程威脅？			□ 適用 □ 不適用 說明：	□ 防範社交工程詐騙宣導說明
4.2.1.6	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？			□ 適用 □ 不適用 說明：	
4.2.2 應訂定執行電子商務作業之電子郵件帳號申請、密碼設定要求等管理規則。					
4.2.2.1	是否牢記並定期更改執行電子商務作業之電子郵件密碼以防止被盜用？			□ 適用 □ 不適用 說明：	
4.2.2.2	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？			□ 適用 □ 不適用 說明：	
4.2.2.3	是否取消自動密碼記憶功能，以避免郵件密碼遭擷取？			□ 適用 □ 不適用 說明：	
4.2.3 應設置防止垃圾郵件或設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件。					
4.2.3.1	是否設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件？			□ 適用 □ 不適用 說明：	□ 郵件過濾規則
4.2.3.2	是否強制所有使用者電子郵件帳號啟用並設定垃圾郵件過濾機制？			□ 適用 □ 不適用 說明：	
4.2.3.3	電子郵件系統如需發送郵件到公司以外之網域，是否考量於郵件本文後加註隱私權、法律責任聲明等，以保障公司權益？		◎	□ 適用 □ 不適用 說明：	
4.3 個人資訊設備安全管理					
4.3.1 應定期進行系統更新，以避免遭受弱點攻擊。					
4.3.1.1	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？			□ 適用 □ 不適用 說明：	□ 作業系統一致更新時程≦1 個月

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.3.2 應制定使用者電腦使用管理規範，要求使用者通行碼、電腦使用、資訊設備操作及工作行為需注意事項。					
4.3.2.1	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？			□ 適用 □ 不適用 說明：	
4.3.2.2	下班時是否登出電腦系統並關閉電源？			□ 適用 □ 不適用 說明：	
4.3.2.3	機房用機、值班用機或是程式執行之限制需常態開機之電腦，是否定期重新開機，以利開機時完成相關修補程式及病毒碼之更新作業，同時避免電腦遭未經授權的存取？		◎	□ 適用 □ 不適用 說明：	
4.3.2.4	是否考量資料安全性，針對桌上型電腦的 USB 連接埠停用大量儲存媒體裝置與軟碟機之使用功能？並建立管制與申請程序。		◎	□ 適用 □ 不適用 說明：	
4.3.2.5	包含敏感或機密資訊的文件是否立即從印表機或傳真機上取走？			□ 適用 □ 不適用 說明：	
4.3.2.6	是否設定作業系統內建之螢幕保護程式，以確保公司資料之安全性？			□ 適用 □ 不適用 說明：	□ 螢幕保護程式設定≦5 分鐘並以密碼保護
4.3.2.7	下班後經辦之機密性及敏感性資訊或文件是否妥為收存？			□ 適用 □ 不適用 說明：	
4.3.2.8	是否定有適當之控制措施，以防止影印機和其他重製技術(例如：掃描器、數位相機)的未經授權使用？		◎	□ 適用 □ 不適用 說明：	
4.3.2.9	是否考量限制將未經授權允許之資訊設備？		◎	□ 適用 □ 不適用 說明：	□ 限制將未經授權允許之資訊設備、軟硬體攜入辦公場所使用 □ 禁止於內部電腦上擅自安裝非公司配發及採購之週邊設備
4.3.2.10	是否建立一般同仁公司配發之電腦遺失或遺失之通報流程與報		◎	□ 適用 □ 不適用	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	案、資產風險控管程序？			說明：	
4.4 網際網路內容瀏覽管理					
4.4.1 應建立網路路由控制，以確保電腦連線與資訊流未違反應用系統之存取控制政策。					
4.4.1.1	是否經由公開機制定期審議Internet內容瀏覽限制、網站過濾規則性？		◎	□ 適用 □ 不適用 說明：	
4.4.1.2	是否有監控網站或過濾網站之運作機制？若有系統或流量異常狀況，應以電話或電子郵件方式告知管理員，並決定是否將其列為資安事件調查。		◎	□ 適用 □ 不適用 說明：	
4.4.2 應限制高風險業務或敏感性資訊避免使用即時通訊軟體或外部電子郵件信箱進行資料傳輸作業。					
4.4.2.1	是否考量限制即時通訊相關軟體(如 MSN, Yahoo 即時通, Google talk)之使用？或監控其記錄與限制傳檔功能？			□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
4.4.2.2	是否考量限制公司外部之電子郵件信箱或 Webmail 之使用？或監控其記錄與限制傳檔功能？			□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
5.強化對外網站交易平台安全管理					
5.1 客戶隱私保護政策宣告作業					
5.1.1 應至少每年審查一次對外公告之隱私權政策，並向所有消費者發布。					
5.1.1.1	是否至少每年一次檢查資訊安全政策及隱私權政策，並在需要時進行更新？			□ 適用 □ 不適用 說明：	□ 查資訊安全政策及隱私權政策發布、更新紀錄
5.1.1.2	是否明確鑑別隱私權相關法令法規要求？			□ 適用 □ 不適用 說明：	□ 隱私權保護聲明 □ 個資蒐集聲明 □ 訂有取得個人資料前，提供當事人取得隱私權聲明之流程
5.1.1.3	是否向所有使用者發布隱私權政策？			□ 適用 □ 不適用 說明：	□ 隱私權保護政策發布紀錄
5.2 交易網站伺服器與網路環境安全管理					
5.2.1 應監視、調諧網路流量、硬碟空間等系統容量的使用與網路連線之狀態，並對未來容量要求預作規劃，以確保所要求之效能。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.2.1.1	是否定時評估網站伺服器上線流量，以維持系統效能需求？			□ 適用 □ 不適用 說明：	□ 系統檢測紀錄
5.2.1.2	資訊相關設備設置前是否進行容量規劃並預留安全容量，並於正式運作時持續監控其容量狀態？			□ 適用 □ 不適用 說明：	□ 容量規畫表 □ 對外交易網站硬碟容量監控紀錄 □ 對外交易網站資料庫容量監控紀錄
5.2.1.3	是否由專人隨時監控網站伺服器的流量，若有異常流量發生時，是否依資訊安全事件處理辦法通報及處置？			□ 適用 □ 不適用 說明：	□ 系統異常事件通報流程
5.2.1.4	是否對於流量負載過重的網站伺服器採取負載平衡機制？		◎	□ 適用 □ 不適用 說明：	
5.2.1.5	是否制定維運規範，以收集可能造成對外交易網站雍塞之災難與預期事件的相關資訊？		◎	□ 適用 □ 不適用 說明：	
5.2.1.6	對外交易網站是否具備偵測網路壅塞並避免網路壅塞時通訊集中之機制？		◎	□ 適用 □ 不適用 說明：	□ 網路偵測機制/設備
5.2.1.7	是否持續監控與其它通信服務互連的狀態？是否有適當的控制措施檢查與其它通訊服務互連是否正常？發生問題時，是否有方法可以檢查？		◎	□ 適用 □ 不適用 說明：	
5.2.1.8	其它通信服務互連是否已妥善定義範圍與介面？是否已定義一旦用戶發生斷線時如何處置的協議或合約？		◎	□ 適用 □ 不適用 說明：	
5.2.2 對外交易網站之網路安全維護上應考量建立連線限制與網路區隔，並架設防火牆或入侵偵測系統。					
5.2.2.1	與交易網站連結的所有路由器、交換器、無線接入點以及防火牆等設備之設定檔資料是否有保護並文件化？			□ 適用 □ 不適用 說明：	
5.2.2.2	是否在交易網站所有邊界路由器或防火牆上設定相關過濾條件，以防止偽造 IP 地址的通過？		◎	□ 適用 □ 不適用 說明：	□ 防火牆規則

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.2.2.3	是否已配置防火牆，並通過網路位址轉換來轉換(隱藏)內部 IP 位址？			□ 適用 □ 不適用 說明：	
5.2.2.4	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？			□ 適用 □ 不適用 說明：	
5.2.2.5	是否考量內部重要網段切割 VLAN？		◎	□ 適用 □ 不適用 說明：	
5.2.2.6	可連上對外網際網路之電腦是否獨立一個網段，與內部含敏感資訊設備之網路分開？		◎	□ 適用 □ 不適用 說明：	
5.2.2.7	對外交易網站管理者是否僅允許在本地端網域中進行連線管理與維護？		◎	□ 適用 □ 不適用 說明：	
5.2.2.8	是否使用入侵偵測系統或入侵防禦系統，以監控對外交易資料環境中的所有流量並在發現可疑威脅時提醒員工？		◎	□ 適用 □ 不適用 說明：	□ IDS □ IPS
5.2.2.9	是否隨時更新所有入侵偵測引擎和入侵防禦引擎？		◎	□ 適用 □ 不適用 說明：	
5.2.2.10	網路中是否使用入侵偵測防護系統並且持續監控 IPS 的警報，並安裝最新的 Signatures？		◎	□ 適用 □ 不適用 說明：	
5.2.3 電子商務線上交易程式或涉及金流與交易相關的應用程式開發，應遵循「2.1 核心營運系統取得、開發及維護安全管理」各項規範要求。					
5.2.3.1	對外交易網站系統取得與開發是否參考「電子商務交易安全規範-網路平台 2.1 核心營運系統取得、開發及維護安全管理」，考量適當查檢項目予以落實？			□ 適用 □ 不適用 說明：	
5.2.4 應設定交易頁面之瀏覽、讀取等限制設定，禁止目錄瀏覽及切換目錄，避免網站目錄內檔案遭竄改或變更。					
5.2.4.1	交易網頁伺服器是否禁止切換回上層目錄？			□ 適用 □ 不適用 說明：	
5.2.4.2	交易網頁伺服器是否禁止目錄瀏覽？			□ 適用 □ 不適用	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
				說明：	
5.2.4.3	使用者對交易網站資料在一般情況下是否僅有「讀取」之權限？			☐ 適用 ☐ 不適用 說明：	
5.2.4.4	網頁伺服器是否規範網頁內容使用語言，並驗證網頁內容之安全性？		◎	☐ 適用 ☐ 不適用 說明：	
5.2.5 應對交易網站所涉及的各項機敏性資料，制定必要的管控政策與措施。					
5.2.5.1	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？			☐ 適用 ☐ 不適用 說明：	
5.2.5.2	是否針對系統內各加密工具制定相關管理政策或使用規範？		◎	☐ 適用 ☐ 不適用 說明：	
5.3 線上交易安全管理					
5.3.1 應有網站交易使用者之帳號管理安全機制，如進行使用者身分認證、強制要求帳號密碼強度等，並記錄帳號申請之核准和撤銷。					
5.3.1.1	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？			☐ 適用 ☐ 不適用 說明：	
5.3.1.2	是否禁止共用帳戶和密碼？			☐ 適用 ☐ 不適用 說明：	
5.3.1.3	是否給予使用者唯一之對應帳號？			☐ 適用 ☐ 不適用 說明：	
5.3.1.4	是否要求使用者使用強度較高的密碼，並建立控管機制？			☐ 適用 ☐ 不適用 說明：	
5.3.1.5	是否建立帳號申請、收回程序與控管機制，並留存相關紀錄留存？			☐ 適用 ☐ 不適用 說明：	
5.3.1.6	對於進行交易的網頁，是否考量採取帳號/密碼以外的客戶身份認證的機制(如信用卡資訊驗證/自然人憑證驗證，或帳號密碼+動態密碼或簡訊或隨機碼驗證或電子郵件驗證)？		◎	☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.3.2 電子商務交易系統應加入查核機制，以預防因作業處理疏失或故意行為所導致之線上交易資訊異常。					
5.3.2.1	是否實施適當之控制措施，以保護在網際網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改？		◎	□ 適用 □ 不適用 說明：	
5.3.2.2	是否制定適當之控制措施以防止線上交易服務的不完整傳輸、誤選路、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演？		◎	□ 適用 □ 不適用 說明：	
5.3.2.3	對於線上交易或申辦服務之公開資訊，是否訂有加密或其他確保機密與完整性之控制措施？			□ 適用 □ 不適用 說明：	
5.3.2.4	是否每日審查與確認對外交易網站之公告訊息與商品資訊正確性？			□ 適用 □ 不適用 說明：	
5.3.2.5	是否建立價格或下單交易異常之預警機制？		◎	□ 適用 □ 不適用 說明：	
5.3.2.6	是否部署相關核心交易系統之檔案完整性監控軟體？如發現未經授權修改重要的系統檔案、組態檔案或內容檔案的操作將提醒員工。		◎	□ 適用 □ 不適用 說明：	
5.3.3 應透過適當之控管措施與安全連線機制(如 SSL 加密等方法)進行交易資料之傳送與傳輸(含資料往返、互換及二次以上傳遞)，以防止未經授權的存取。					
5.3.3.1	對於採用語音、傳真、網路或視訊通訊等設施進行電子商務供應鏈交易資訊交換，是否採取加密傳輸或保護控制措施？			□ 適用 □ 不適用 說明：	
5.3.3.2	公司與任何電子商務產業供應鏈間資訊與軟體的交換，是否訂有適當的交換政策、協議、程序或控制措施，以保護經由使用所有形式之通信設施的資訊交換？			□ 適用 □ 不適用 說明：	□ 備有資料交換協議
5.3.3.3	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、誤用或毀損？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.3.3.4	重要電腦資訊、儲存媒體之運送，是否有安全保護措施並留有完整監控紀錄(含收送人、時間及內容)？		◎	☐ 適用 ☐ 不適用 說明：	
5.3.3.5	透過電子郵件傳送包含帳號或電子商務交易之敏感資訊時，是否進行加密？		◎	☐ 適用 ☐ 不適用 說明：	
5.3.3.6	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)？			☐ 適用 ☐ 不適用 說明：	
5.3.3.7	採行電子交換之資訊是否視安全等級採行帳號與通行碼管制、電子資料加密或電子簽章認證等保護措施，以確保資訊的可用性、完整性、機密性及其他法律考量？		◎	☐ 適用 ☐ 不適用 說明：	
5.3.3.8	網站交易服務是否有受到例如SSL/TLS或IPSEC等方法之加密保障？(如 SSL 加密強度是否達 128 位元以上？)		◎	☐ 適用 ☐ 不適用 說明：	
5.3.3.9	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？			☐ 適用 ☐ 不適用 說明：	☐ 加密機制：_____
5.3.4 敏感性資料(如身份證字號、信用卡卡號等資訊)於交易畫面顯示時，應遮蔽並透過加密機制傳輸，避免資料遭竊取。					
5.3.4.1	顯示持卡人資料時，除了帳號的最後 4 位外，是否無法看到其他所有的數字？		◎	☐ 適用 ☐ 不適用 說明：	
5.3.4.2	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？			☐ 適用 ☐ 不適用 說明：	
5.3.4.3	是否禁止 Web 交易頁面程式提供網頁重新導向功能，讓使用者可透過該程式連接到其他網站？		◎	☐ 適用 ☐ 不適用 說明：	
5.3.4.4	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)？			☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.3.4.5	交易頁面是否通過相關檢核驗證機構認證？(如 TWCA、PCIDSS、ISO27001 等認證)		◎	□ 適用 □ 不適用 說明：	
5.3.5 應透過密碼、檔案加密工具或金鑰針對儲存之交易資料進行加密。					
5.3.5.1	是否安全的加密方式儲存(在資料庫、日誌檔、備份介質中)帳號？		◎	□ 適用 □ 不適用 說明：	
5.3.5.2	敏感的持卡人資料是否儲存在安全或已加密的 Cookie 中？		◎	□ 適用 □ 不適用 說明：	
5.3.5.3	是否考量對所有網路設備和系統的通行碼進行加密？		◎	□ 適用 □ 不適用 說明：	
5.3.5.4	是否對交易網站機敏性資料(或資料庫)及交易資料庫進行加密處理？金鑰是否異地進行存放？		◎	□ 適用 □ 不適用 說明：	
5.3.6 交易資料庫應禁止留存客戶信用卡卡號、驗證碼，並不將個人資料等敏感訊息存於公開之網頁伺服器。					
5.3.6.1	是否禁止在資料庫、日誌檔或 POS 系統中儲存信用卡驗證碼？		◎	□ 適用 □ 不適用 說明：	
5.3.6.2	是否未將客戶資料及任何信用卡資料儲存在公開的網頁伺服器？		◎	□ 適用 □ 不適用 說明：	
5.3.7 應留存對外交易網站之交易與信用卡資料存取交易紀錄，並定期審查交易網站相關設備(含主機、網路設備、資料庫等...)之日誌資訊。					
5.3.7.1	是否留存使用者操作與網路交易之紀錄？			□ 適用 □ 不適用 說明：	
5.3.7.2	是否定期追蹤和監控金融交易資料的異常操作？		◎	□ 適用 □ 不適用 說明：	
5.3.7.3	是否對所有持卡人資料的存取(包括 Administrator/Supervisior 的訪問)進行記錄？			□ 適用 □ 不適用 說明：	
5.3.7.4	持卡人資料存取記錄是否包含成功或失敗的登錄嘗試及資料庫紀錄？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.3.7.5	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？			☐ 適用 ☐ 不適用 說明：	
5.4 交易網站技術弱點管理					
5.4.1 對外交易網站應修改預設參數，並建立網站攻擊手法之預防機制。					
5.4.1.1	是否將對外網站伺服器各項系統設定與預設參數修改為安全建議值？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.1.2	是否對 Web 程式提供的檔案讀取功能參數進行檢查，確認對外公開的重要檔案與目錄不可被任意存取？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.1.3	是否對 Web 程式進行安全組態設定確認？			☐ 適用 ☐ 不適用 說明：	☐ 預設帳號或變更密碼 ☐ 安全性更新 ☐ 重要資料目錄保護
5.4.1.4	是否針對系統參數操作的安全需求，進行常見攻擊手法及控管機制的評估，並建立參數操作檢測機制與落實防護？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.1.5	是否針對由使用者輸入之參數，使用適當檢測機制與防護措施檢核，並留存相關紀錄？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.1.6	是否對於新的攻擊手法，建立適合的授權檢查機制與防護方法？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.1.7	是否對於新的攻擊手法，設計稽核紀錄的留存以備後續之內容分析？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.1.8	是否對於新的攻擊手法，調整系統內部的相關設定與參數，增補適當的檢查機制？		◎	☐ 適用 ☐ 不適用 說明：	
5.4.2 對外交易網站應定期實施各式技術性弱點測試，以強化電子商務交易服務安全。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.4.2.1	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？			□ 適用 □ 不適用 說明：	□ 程式原始碼檢測 □ 弱點掃描檢測 □ 滲透測試檢測
5.4.2.2	是否針對 Web 程式進行原始碼掃描測試以降低遭受攻擊之風險(例如 SQL Injection、Cross Site Scripting 等攻擊手法)？		◎	□ 適用 □ 不適用 說明：	
5.4.2.3	伺服器端的控制能否防止 SQL Injection 攻擊和其他繞過用戶端 Scripts 控制的攻擊？		◎	□ 適用 □ 不適用 說明：	
5.4.2.4	是否針對 Web 程式的身分驗證與連線管理等功能進行身分與權限操作測試？		◎	□ 適用 □ 不適用 說明：	
5.4.2.5	是否於 Web 程式禁止使用者加入連結或指令碼進行系統操作，或修改系統設定？		◎	□ 適用 □ 不適用 說明：	
5.4.2.6	是否限制 Web 程式權限的控管(特別針對後台界面)，禁止透過修改 url 路徑或參數，來存取包含有機敏資訊或管理權限的頁面？		◎	□ 適用 □ 不適用 說明：	
6. 建立資安通報管理機制					
6.1 電子商務資安通報機制					
6.1.1 電子商務網路平台應參照電子商務資安通報機制規範，進行資安事故外部通報。					
6.1.1.1	是否參考電子商務資安通報機制規範，建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常等)之外部通報與提報程序？		◎	□ 適用 □ 不適用 說明：	
6.1.1.2	是否具體落實外部通報作業？			□ 適用 □ 不適用 說明：	
6.1.1.3	是否隨時接收外部重大資安資訊，並立即採取必要反應行動？			□ 適用 □ 不適用 說明：	
6.2 資安事故管理					
6.2.1 應建立資安事故通報管理程序，並對內外部員工宣導相關通報流程。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
6.2.1.1	是否建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常等)之事件通報與提報程序？			□ 適用 □ 不適用 說明：	
6.2.1.2	員工及外部使用者是否知悉資安事件通報及處理程序並依規定辦理？			□ 適用 □ 不適用 說明：	□ 公告資安事件通報程序 □ 辦理人員認知訓練
6.2.1.3	是否要求資訊系統與服務的所有員工、產業供應鏈上下游業者及第三方使用者，注意並通報系統或服務之任何觀察到或可疑的安全弱點？			□ 適用 □ 不適用 說明：	
6.2.1.4	是否建立資訊安全事件通報的聯絡點，確保全組織都知道該聯絡點，隨時可聯繫，並能夠有充分與及時的回應？		◎	□ 適用 □ 不適用 說明：	□ 聯絡清單公告地點：_____
6.2.2 應界定人員緊急應變的責任，以確保對資訊安全事故做迅速、有效及依序的回應。					
6.2.2.1	是否建立資安事件之通報及事故回應與提報處理程序的管理責任與職掌定義？			□ 適用 □ 不適用 說明：	
6.2.2.2	是否依不同型式的資訊安全事故，建立資安事故管理責任及應變程序？			□ 適用 □ 不適用 說明：	
6.2.3 應建立相關紀錄與證據管理之相關程序，以完整收集、保存資安事故之證據，且日後可取出供查驗，同時可針對事故之原因進行檢討分析。					
6.2.3.1	是否建立資安事故管理機制，如記錄事故型式、處置方法、處理成本及矯正預防措施？			□ 適用 □ 不適用 說明：	
6.2.3.2	是否辦理資安事件或事故後之檢討會議，以協助單位能從資安事件、事故中學習？			□ 適用 □ 不適用 說明：	
6.2.3.3	是否已建立及使用各項指標，以協助偵測安全事件，並預防安全事故？		◎	□ 適用 □ 不適用 說明：	
6.2.3.4	已發生之資訊安全事故是否在資訊安全政策審查過程中納入考量？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
6.2.3.5	資安事件中相關證據資料是否有適當保護措施以作為問題分析及法律必要依據？			□ 適用 □ 不適用 說明：	
6.2.3.6	資安事件之回應小組是否被授權在處理事件時採取立即之決定？		◎	□ 適用 □ 不適用 說明：	□ 備有授權文件或相關辦法
6.2.3.7	資安事件之回應小組是否與外部團體(例如：執法機關、政府緊急應變中心、客戶、產業供應鏈上下游業者、電子商務資安事件通報機制等)建立一定之聯繫管道？		◎	□ 適用 □ 不適用 說明：	□ 備有外部聯絡清單 - 執法機關 - 政府緊急應變中心 - 客戶 - 產業供應鏈上下游業者
6.2.3.8	資訊安全事件處理的過程是否均留有完整紀錄？如有必要，應經由直接發送的電子郵件或網站首頁即時回報事件予相關產業供應鏈上下游業者與消費者。		◎	□ 適用 □ 不適用 說明：	□ 資安事件報告單

資料來源：本計畫整理

陸、附錄

一、參考文件索引表

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
策略目標：1.促進組織資訊安全管理			
1.1 資訊安全框架	1.1.1	ISO 27001 A5	
		ISO 27001 4.3	
		ISO 27001 8	
		ISO 27001 6	
		ISO 27001 4.2	
	1.1.2	ISO 27001 A.6.1.1	
		ISO 27001 A.6.1.2	
		ISO 27001 A.6.1.3	
		ISO 27001 A.6.1.4	
		ISO 27001 A.6.1.5	
		ISO 27001 A.6.1.6	
		ISO 27001 A.6.1.7	
		ISO 27001 A.6.1.8	
1.2 風險管理	1.2.1	ISO 27001 4.2	
		ISO 27001 A.6.1.3	
		ISO 27001 4.2.1(d) (1)	
		ISO 27001 A7.1.2	
		ISO 27001 4.2.1(d) (2)	
		ISO 27001 4.2.1(d) (3)	
		ISO 27001 4.2.1(e) (1)	
		ISO 27001 4.2.1(c)	
		ISO 27001 4.2.1(e) (2)	
		ISO 27001 4.2.1(e) (3)	
	1.2.2	ISO 27001 4.2.2(a)	
		ISO 27001 4.2.2(b)	
		ISO 27001 4.3.1(e), ISO 27001 4.2.1(c) (2)	
1.3 資訊資產管理	1.3.1	ISO 27001 A.7.1.1	
	1.3.2.	ISO 27001 4.2.1(d) A.7.1.2	
		ISO 27001 A.7.1.3	
		ISO 27001 A.7.2.1	
		ISO 27001 A.7.2.2	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
1.4 人力安全管理	1.4.1	ISO 27001 A.8.1.1	ISO 27011
		ISO 27001 A.8.1.2	ISO 27011
		ISO 27001 A.8.1.3	
		ISO 27001 A.8.2.3	
	1.4.2	ISO 27001 A.8.2.1	
		ISO 27001 A.8.2.2	
		ISO 27001 A.8.3.2 ISO 27001 A8.3.1	
		ISO 27001 A.8.3.3	
1.5 遵循性管理	1.5.1	ISO 27001 A.15.1.1	
		ISO 27001 A.15.1.4	「客戶資料保護準則」
		ISO 27001 A.15.2.1	
	1.5.2	ISO 27001 A.15.1.2	
	1.5.3.	ISO 27001 A.15.1.3	
		ISO 27001 A.15.1.5	
		ISO 27001 A.15.2.2	
		ISO 27001 A10.10.3	
1.6 委外管理	1.6.1.	ISO 27001 A.6.2	
		ISO 27001 A.10.2.3	
		ISO 27001 A.10.2.1	
		ISO 27001 A.10.2.2	
		ISO 27001 A.6.1.5	
	1.6.2	ISO 27001 A.6.2	
		ISO 27001 A15.1.4	
		ISO 27001 A.11.2	
		ISO 27001 A.6.2.1	
	1.6.3.	ISO 27001 A6.1.5	
		ISO 27001 A.6.2	
	1.6.4	ISO 27001 A6.1.5	
		ISO 27001 A.6.2	
策略目標：2.加強核心營運系統與資料庫之安全管理			

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
2.1 核心營運系統取得、開發及維護安全管理	2.1.1	ISO 27001 A.12.1	
	2.1.2	ISO 27001 A.12.2.2	
		ISO 27001 A.12.2.1	
	2.1.3	ISO 27001 A.12.4.1	
		ISO 27001 A.12.5.2	
	2.1.4	ISO 27001 A.12.4.2	
		ISO 27001 A.12.5.4	ISO 27011
	2.1.5	ISO 27001 A.12.4.3	ISO 27011
		ISO 27001 A.12.5	ISO 27011
	2.1.6	ISO 27001 A.12.5.1	ISO 27011
		ISO 27001 A.12.5.2	
		ISO 27001 A.12.5	
		ISO 27001 A.10.3.2	
		ISO 27001 A.12.5.5	
		ISO 27001 A.12.6.1	
2.2 核心營運系統存取控制管理	2.2.1	ISO 27001 A.11.2.1	
		ISO 27001 A.11.2.2	
		ISO 27001 A.11.2.3 , A.11.4.2	
		ISO 27001 A.11.5.1	
	2.2.2	ISO 27001 A.11.4.2	
		ISO 27001 A.11.2.3	
		ISO 27001 A.11.5.2	
		ISO 27001 A.11.2.3	
		ISO 27001 A.11.2.4	
		ISO 27001 A.11.5.3	
		ISO 27001 A.11.3.1	
		ISO 27001 A.11.5.1	
	2.2.3	ISO 27001 A.11.3.3	
		ISO 27001 A.11.3.2	
	2.2.4	ISO 27001 A.11.4.5	
		ISO 27001 A.11.4.6	
		ISO 27001 A.11.4.7	
		ISO 27001 A.11.6.2	
		ISO 27001 A.11.4.1	
		ISO 27001 A.11.4.3	
		ISO 27001 A.11.4.2	
		ISO 27001 A.11.7.2	
	2.2.5	ISO 27001 A.11.5.4 ISO 27001 A.11.4.6	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
		ISO 27001 A.11.7.2	
	2.2.6	ISO 27001 A.11.5.5	
		ISO 27001 A.11.5.6	
2.3 核心營運系統機房與作業環境實體安全	2.3.1	ISO 27001 A.9.1.1	ISO 27011
		ISO 27001 A.11.2.4	
		ISO 27001 A.9.1.2	ISO 27011
		ISO 27001 A.9.2	ISO 27011
		ISO 27001 A.9.1.4	ISO 27011
		ISO 27001 A.9.1.5	
	2.3.2	ISO 27001 A.9.1.1	
		ISO 27001 A.9.1.4	ISO 27011
		ISO 27001 A.9.1.5 ISO 27001 A.9.2.7	
		ISO 27001 A.9.1.6	
	2.3.3	ISO 27001 A.9.2.1	
		ISO 27001 A.9.2.2	
		ISO 27001 A.9.2.3	
		ISO 27001 A.9.2.4	
	2.3.4	ISO 27001 A.11.3.2	
		ISO 27001 A.9.2.5	
	2.3.5	ISO 27001 A.9.2.6	
		ISO 27001 A.9.2.5	
		ISO 27001 A.9.2.7	
2.4 核心營運系統資料庫安全管理	2.4.1	ISO 27001 A.11.4.5	PCI-DSS 1.3.7
		ISO 27001 A.11.4.7	
		ISO 27001 A.12.4.2	
		ISO 27001 A.11.6.2	PCI-DSS 2.2.1
		ISO 27001 A.11.6.1	PCI-DSS 3.4.1
		ISO 27001 A.12.6.1	PCI-DSS 6.1
		ISO 27001 A.12.5.4	
	2.4.2.	ISO 27001 A.10.3.1	
		ISO 27001 A.10.3.1	
		ISO 27001 A.10.3.1	
		ISO 27001 A.13.2.1	BS25999
		ISO 27001 A.10.3.1 ISO 27001 A.10.10.2	
		ISO 27001 A.11.6.1	PCI-DSS 8.5.16
	2.4.3	ISO 27001 A.10.5.1	PCI-DSS 9.5
	2.4.4	ISO 27001 A.10.10.3, A.10.10.4	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
2.5 核心營運系統營運持續安全管理	2.5.1	ISO 27001 A.14.1.2	BS 25999
		ISO 27001 A.14.1.3	BS 25999
		ISO 27001 A.14.1	
		ISO 27001 A.14.1.5	
策略目標：3.強化客戶個人資料安全管理			
3.1 客戶資料隱私管理	3.1.1	ISO 27001 A.15.1.4	
	3.1.2	個資法第 18 條	BS 10012 4.1
	3.1.3		BS 10012 4.10
	3.1.4		BS 10012 4.4
3.2 客戶資料盤點作業	3.2.1	ISO 27001 A7.1.1	BS 10012 4.2
		ISO 27001 A7.2.1	BS 10012 4.2
			BS 10012 4.13
3.3 客戶資料依法對外公開、資訊揭露作業	3.3.1		BS 10012 4.15
	3.3.2		BS 10012 4.1
3.4 客戶資料蒐集、處理及儲存管理作業	3.4.1	個資法第 19 條	
		個資法第 6 條	
		個資法第 8 條	
		個資法第 3 條	BS 10012 4.10
		個資法第 10 條	
		個資法第 9 條	
	3.4.2.	ISO 27001 A8.2.2	BS 10012 4.3
	3.4.3.	ISO 27001 A10.2.1	BS 10012 4.15
		ISO 27001 A6.1.5	
	3.4.4		BS 10012 4.1
			BS 10012 4.2
		ISO 27001 A.8.1.3	
		ISO 27001 A.8.3.3	
		ISO 27001 A.11.3.1	
		ISO 27001 A.11.2	
		ISO 27001 4.2.4	
		ISO 27001 A.11.2.1	
		ISO 27001 A.10.10	
	3.4.5	ISO 27001 A.10.7	
		ISO 27001 A.9.2.1	
		ISO 27001 A.9.2.7	
		ISO 27001 A.10.8.3	
		ISO 27001 A.9.1.2	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
		ISO 27001 A.11.6.2	
		ISO 27001 A.10.4.1	
		ISO 27001 A.12.6.1	
		ISO 27001 A.11.7.1	
		ISO 27001 A.10.7.1	BS 10012 4.13
3.5 客戶資料使用及傳輸安全作業	3.5.1	個資法第 11 條	BS 10012 4.8
		個資法第 5 條	
	3.5.2	ISO 27001 A.10.2	BS 10012 4.16
		ISO 27001 A.10.8.2	BS 10012 4.13.3
	3.5.3	ISO 27001 A.10.7.4	
		ISO 27001 A.10.8	
		ISO 27001 A.10.8.1	
		ISO 27001 A.11.1	
		ISO 27001 A.10.10.1	
		ISO 27001 A.10.7.3, A.11.6.2	
		ISO 27001 A.11.1	
			BS 10012 4.2
			BS 10012 4.9
			BS 10012 4.9
		ISO 27001 A.10.10.4	
3.6 客戶資料正確性維護作業	3.6.1		BS 10012 4.10
	3.6.2		BS 10012 4.12
	3.6.3	ISO 27001 A.12.2	BS 10012 4.10
	3.6.4	個資法第 3 條	BS 10012 4.10
3.7 客戶資料刪除及停止利用作業	3.7.1	ISO 27001 A.10.7.2	
	3.7.2	ISO 27001 A.10.7.4	
		ISO 27001 A.10.8	BS 10012 4.13
	3.7.3	ISO 27001 A.10.7	
	3.7.4	ISO 27001 A.10.5	
策略目標：4.提升企業內資訊環境安全管理			
4.1 網路通訊與資訊作業安全管理	4.1.1	ISO 27001 A.10.1.1	
		ISO 27001 A.10.1.2	
		ISO 27001 4.3	
	4.1.2	ISO 27001 A.10.1.3	
		ISO 27001 A.12.5.1	
		ISO 27001 A.10.1.4	
	4.1.3	ISO 27001 A.10.7.1	
		ISO 27001 A.10.4.1	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
		ISO 27001 A.10.4.2	ISO 27011
	4.1.4	ISO 27001 A.10.5.1	
		ISO 27001 A.9.1.2	
		ISO 27001 A.9.1.4	
		ISO 27001 A.9.1.1	
	4.1.5	ISO 27001 A.10.6.1	OWASP 4.4 (OWASP-AT-001-010)
		ISO 27001 A.10.6.2	ISO 27011
		ISO 27001 A.10.6	ISO 27011
	4.1.6	ISO 27001 A.10.6	
		ISO 27001 A.11.4.4	
		ISO 27001 A.11.4	
		ISO 27001 A.11.4.2	
		ISO 27001 A.11.5.2, A.11.6.1	
		ISO 27001 A.11.7.1	
		ISO 27001 A.12.4.1	
	4.1.7	ISO 27001 A.10.10.1	
		ISO 27001 A.10.10.2	
		ISO 27001 A.10.10.3	
		ISO 27001 A.10.10.4	
		ISO 27001 A.10.10.5	
	4.1.8	ISO 27001 A.10.10.6	PCIDSS 10.4
			「電子商務安全人才培訓與輔導計畫：安全偵測機制控制項」
4.2 電子郵件安全管理	4.2.1	ISO 27001 A.10.8.4	
		ISO 27001 A.10.6, A.10.8.2	
		ISO 27001 A.10.8	
		ISO 27001 A.10.6.1	
		ISO 27001 A.8.2.2	
		ISO 27001 A.10.4.1	
	4.2.2	ISO 27001 A.11.2.3	
		ISO 27001 A.11.3.1	
		ISO 27001 A.10.6	
	4.2.3	ISO 27001 A.10.6	
4.3 個人資訊設備安全管理	4.3.1	ISO 27001 A.10.1.2 ISO 27001 A.12.6.1	
	4.3.2	ISO 27001 A.11.3.1	
		ISO 27001 A.11.3.3	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
		ISO 27001 A.10.1.2	
		ISO 27001 A.10.7.1	
		ISO 27001 A.6.1.4, A.7.1.3	
		ISO 27001 A.15.1.5	
4.4 網際網路內容瀏覽管理	4.4.1	ISO 27001 A.10.6, A.11.4	
	4.4.2	ISO 27001 A.10.8.4, A.11.4.1	
策略目標：5.強化對外網站交易平台安全管理			
5.1 客戶隱私保護政策宣告作業	5.1.1	ISO 27001 7.1	BS10012 3.4、PCIDSS R12
		BS10012 4.7	
		ISO 27001 A.15.1.4	PCIDSS R12
		個資法第 8 條	BS10012 4.7.3
5.2 交易網站伺服器與網路環境安全管理	5.2.1	ISO27001 A.10.3.1	
		ISO27001 A.10.10.2	
		ISO27001 A.13.1.1	
		ISO27001 A.10.3.1	
		ISO 27001 A.14.1	ISO 27011
		ISO 27001 A.10.6	ISO 27011
	5.2.2	ISO 27001 A.10.7.4	PCIDSS R1.R2
		ISO 27001 A.11.4.6	PCIDSS R1.R2
		ISO 27001 A.10.6.1	PCIDSS 1.2.3
		ISO 27001 A.11.4.5	PCIDSS R1.R2
		ISO27001 A.10.10.2	
		ISO 27001 A.11.7.2	
		ISO 27001 A.10.6.2	
	5.2.3	ISO 27001 A.10.6 ISO27001 A.10.9.1	
	5.2.4	ISO 27001 A.10.10.1	
		ISO 27001 A.11.6.1	PCIDSS 7.2.2
		ISO 27001 A.11.6.2	PCIDSS 2.2.1
		ISO 27001 A.12.3.1	
	5.2.5	ISO 27001 A.10.10.1	
		ISO 27001 A.10.1.3	
		ISO27001 A.10.5.1	
5.3 線上交易安全管理	5.3.1	ISO 27001 A.11.4.2	PCIDSS R7.R8.R9
		ISO 27001 A.11.3.1	PCIDSS R7.R8.R9
		ISO 27001 A.11.5.2	
		ISO 27001 A.11.5.1	

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
		ISO 27001 A.11.2.1	
		ISO 27001 A.10.9.2	PCIDSS 10.2.5
	5.3.2	ISO 27001 A.11.4.2, A.11.5.1	PCIDSS R7.R8.R9
		ISO 27001 A.11.3.1	PCIDSS R7.R8.R9
		ISO 27001 A.11.5.2	
		ISO 27001 A.12.2.4	
		ISO 27001 A.11.2.1	
		ISO 27001 A.10.9.2 ISO 27001 A.10.10.2	PCIDSS 10.2.5
	5.3.3	ISO 27001 A.10.8.1	PCIDSS 2.1.1
		ISO 27001 A.10.8.2	
		ISO 27001 A.10.7.1	
		ISO 27001 A.10.8.3, A.10.10.1	
		ISO27001 A.10.8.4	PCIDSS R3.R4
		ISO27001 A.12.3.1	
		ISO 27001 A.15.1.6	
			PCIDSS 4.1
	5.3.4	ISO 27001 A.10.8.1	PCIDSS 2.1.1
		ISO 27001 A.10.8.2	
		ISO 27001 A.10.8.3	
		ISO 27001 A.10.10.1	
		ISO27001 A.10.8.4,	PCIDSS R3.R4
		ISO 27001 A.15.1.4	
		ISO 27001 A.15.1.6	
			PCIDSS 4.1
		ISO 27001 A.12.3.1	PCIDSS R3.R4
	5.3.5	ISO 27001 A.12.5.4	PCIDSS R3.R4
		ISO 27001 A.10.6.1	PCIDSS R1.R2
		ISO 27001 A.10.6.2	OWASP 2010 Top 10
		ISO 27001 A.10.9.2	
		ISO 27001 A.15.1.4	
	5.3.6.	ISO 27001 A.12.3.1	PCIDSS R3.R4
		ISO 27001 A.15.1.4	PCIDSS R5.R6
		ISO 27001 A.12.3.1	PCIDSS R7.R8.R9
		ISO 27001 A.12.3	OWASP 2010 Top 10
	5.3.7	ISO 27001 A.10.9.2 ISO 27001 A.10.10.1	PCIDSS R3.R4
		ISO 27001 A.10.10.2	PCIDSS 3.2.2

管理項目	要求之查檢項目	依據之法規或標準	其他可供規範實作之參考
	5.3.8	ISO 27001 A.10.10.5	
		ISO 27001 A.10.10.1	PCIDSS R10.R11
		ISO 27001 A.10.10.2	
5.4 交易網站技術弱點管理	5.4.1	ISO 27001 A.9.2.4	
		ISO 27001 A.11.2.4	OWASP 2010 Top 10
		ISO 27001 A.15.2.2	
		ISO 27001 A.12.6	
		ISO 27001 A.10.10.1	
		ISO 27001 A.12.2.1	
	5.4.2.	ISO 27001 A.12.6	PCIDSS R10.R11
		ISO 27001 A.15.2.2	OWASP 2010 Top 10
		ISO 27001 A.11.2.4	PCIDSS R5.R6
策略目標：6. 建立資安通報管理機制			
6.1 電子商務資安通報機制	6.1.1	ISO 27001 A.13.1	「電子商務資安通報機制規範與作業要點」
		ISO 27001 A.13.2.1	
6.2 資安事故管理	6.2.1	ISO 27001 A.13.1	
		ISO 27001 A.6.1.6	
	6.2.2	ISO 27001 A.13.2	
	6.2.3	ISO 27001 A.13.2	
		ISO 27001 8.3	
		ISO 27001 8.2	

二、規範常見名詞釋義

項次	名詞	定義說明	備註
1	風險評鑑	風險分析與風險評估的整個過程。	
2	風險	威脅利用弱點對資訊資產所造成影響之可能性。	
3	風險評估	把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。	
4	風險分析	系統性的使用資訊，以識別緣由與估計風險。	
5	威脅	危及資訊資產的外在因素，如天然災害、惡意攻擊等。	
6	脆弱點	指資訊資產內部可能遭受威脅利用之處。	
7	螢幕淨空	當設備無人看管或使用時宜將個人電腦和終端機保持在登出或鎖定狀態，以通行碼等授權機制保護的螢幕及鍵盤上鎖機制保護。	

項次	名詞	定義說明	備註
8	惡意程式、惡意碼	故意建立用來執行未經授權並通常是有害行為的軟體程序，包括病毒、後門程序、鍵盤紀錄器、密碼盜取者和其它木馬程序、Word 和 Excel 病毒、木馬、犯罪軟體、間諜軟體和廣告軟體。	
9	行動碼	由遠端系統透過網路轉存入本機端進行代理作業，可進行下載或在本機端上執行沒有明確安裝或者接受者的作業。包括 include scripts(Java 腳本，VBScript)、Java 小應用程式，ActiveX 控制，flash 動畫。	
10	安全容量	系統或網路的資源使用宜監控、調校、及預估未來容量需求，以確保服務可有效運作。	
11	時間同步	業務營運相關系統宜與議定的準確時間(如中原標準時間、NTP 或其他公正單位)進行時間校正與同步作業。	
12	委外廠商	第三方委外單位、第三方合作業者，含物流商、供應商及服務商等。	
13	利害相關團體	執法機關、政府緊急應變中心、客戶、產業供應鏈上下游業者、電子商務資安事件通報機制。	
14	儲存媒體	資料儲存媒介，例如：紙本文件、電腦媒體(磁片、磁帶、記憶卡、外接硬碟與光碟片)。	
15	可攜式設備	包括筆記型電腦、PDA 等。	
16	密碼、加密	Cryptographic，將正常的(可識別的)資訊轉變為無法識別的信息。	
17	通行碼	Password，對應帳號的登入密碼，使用者在存取資訊系統與服務前，依使用者授權用來查證其身份的方法。	
18	資訊安全事件	information security event 系統、服務或網路狀態經鑑別而顯示示可能有違反資訊安全政策或保護措施失效，或可能與安全有關但事先未知狀況的發生。	
19	TWCA	臺灣網路認證公司，提供國內網路安全認證服務，為國內最大的民間憑證發行機構。	
20	PCIDSS	Payment Card Industry Data Security Standard，支付卡產業相關標準指引與要點，由 Visa International、MasterCard Worldwide、 American Express、Discover Financial Services 及 JCB 等支付卡產業安全標準委員會提出，目的在幫助公司保護支付卡帳戶資料。	1.2.1 版，2009 年 7 月版
21	保密協議	透過保密切結書、合約書等文件規範相關保密要求。	參照 ISO 27002-6.1.5

項次	名詞	定義說明	備註
22	社交工程	利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。	
23	即時通訊軟體	如 msn、yahoo 即時通、Google Talk、Skype 等軟體，可使用網路即時的傳遞文字訊息、檔案、語音與視訊交流。	

供應商交易安全規範

經濟部商業司

電子商務交易安全規範
供應商
規範、進階指引及查檢表

V3.0 版

指導單位：經濟部商業司
主辦單位：財團法人資訊工業策進會
執行單位：中華無店面商務發展協會
中 華 民 國 １０１ 年 １０ 月

目　錄

圖目錄

表目錄

壹、前言

一、依據

經濟部商業司(下稱商業司)「101 年度電子商務交易安全及資安服務平台推動計畫」(下稱本計畫)。

二、主旨

為提升電子商務供應鏈之電子商務平台業者之資訊安全管理、商品供應商(或賣家)的資訊管理與物流商資訊管理流程等之作業安全需求，特召集產業代表、專家學者、顧問單位共同參與規劃、審查並修正「電子商務交易安全規範」(下稱本規範)，做為我國電子商務產業相關業者之行政參考文件，本規範依實施對象分別編纂 3 份規範文件：

(一) 電子商務交易安全規範-網路平台 1 式

(二) 電子商務交易安全規範-供應商 1 式

(三) 電子商務交易安全規範-物流商 1 式

以有助於電子商務業者致力提升交易安全、強化消費者安全信賴時，於各項管理面、作業面之實務參考。

三、電子商務定義

我國行政院主計總處所編印之「中華民國行業標準分類」，其主要目的在於提供統計分類之用，行業標準分類原則主要係參酌聯合國國際行業標準分類(International Standard Industrial Classification of All Economic Activities, ISIC)中以場所單位之主要經濟活動作為分類基礎之架構。其中關於電子商務之定義，依據聯合國國際行業標準分類第 4 次修訂版(ISIC Rev.4)之定義為:「企業單位接到訂單後，以各種電子媒介方式處理所生產之商品及服務之交易，例如藉由電話、傳真、電視、電子資料交換(EDI)及網際網路。」亦即所有從事

商品或服務之所有權移轉，是藉由網際網路或其他的電子媒介所為的商業交易行為就稱之為電子商務。

另依據商業司在「2011 電子商務年鑑」，將電子商務定義為：「運用先進資訊科技，同時藉由組織作業的流程改造，來達到減低組織營運的成本開支，提升作業效率，增加客戶滿意度之商業活動。」亦即利用電腦或新興手持式電子產品，例如智慧型手機、平版電腦等，透過網路進行買賣交易之行為皆稱之為「電子商務」。如商業 EDI(Electronic Data Interchange)、金融 EDI、網路銀行、網路購物等行為，都涵蓋在電子商務範疇之中。

四、目的

本規範文件之制定，除參考我國資通安全管理相關規範、CNS 27001:2005 資訊安全管理標準、個人資料保護法及其他國際標準中與電子商務產業相關的規範，據以規劃本規範文件之框架，並依據以下目的，訂定適合企業交易安全實務操作之文件。

(一) 依電子商務業者之營業額、個資量、作業特性等分級分類，不同等級給予不同的資安防護實施建議。

(二) 3 份交易安全規範，至少涵蓋以下作業流程，以利電子商務業者掌握上下游作業之資訊安全。

1. 電子商務供應鏈之中大型電子商務平台業者之資訊安全管理。
2. 含內部資訊流管理。
3. 交易網站安全機制管理。
4. 有效的交易網站安全機制。
5. 與供應鏈的協同資訊作業管理。

6. 商品供應商(或賣家)的資訊管理(含交易資訊管理流程)。

7. 物流商資訊管理流程(含客戶資料保護管理)。

8. 作業安全需包含交易資訊之機密性、交易平台之可用性、交易內容之完整性、與交易作業之適法性等需求。

貳、文件說明

一、適用範圍

(一)「電子商務交易安全規範-網路平台」適用對象為電子商務平台業者，其類型包含如下，並不加以第一類、第二類區分，規範要求皆適用。

1. B2C 平台商：使用電子商務技術，直接提供消費者商品購買服務之廠商。

2. B2B2C 平台商：提供網路交易平台，由個別網路商家參與，使用電子商務技術，直接或間接提供消費者購買服務之廠商。

(二)「電子商務交易安全規範-供應商」適用對象為配合網路平台電子商務交易，提供直接或間接 B2C 商品經銷或銷售之代理業者、經銷業者、零售業者或電子商家。不涉入 B2C 商品交易之訂購服務、客服服務、金流作業、配送服務等流程之商品製造、輸入、代理、經銷或銷售等業者，不包含在本規範之適用範圍中。

1. 第一類供應商：只擁有一般網際網路連線、使用一般網站(Web)交易系統及一般辦公室使用之 OA 電腦設備之供應商。

2. 第二類供應商：擁有或租賃或委外之網際網路專線、營運系統或其他與電子商務相關應用系統之供應商，或與網路平台、物流商之間，透過後台連線交換傳遞或拋轉客戶之會員資料、訂購資料、交易金額、配送資料之供應商。

(三)「電子商務交易安全規範-物流商」適用對象為配合網路平台電子商務交易，提供直送或轉運 B2C 境內(含離島)商品配送服務流程之汽機車快遞業者、路線貨運業者、宅配業者、郵遞業者，

以及提供取貨服務之實體商店等。跨境之海陸空運承攬業者、倉儲流通轉運業者、大型批發物流流通業者等不涉入 B2C 商品配送服務的作業流程，不包含在本規範適用範圍。

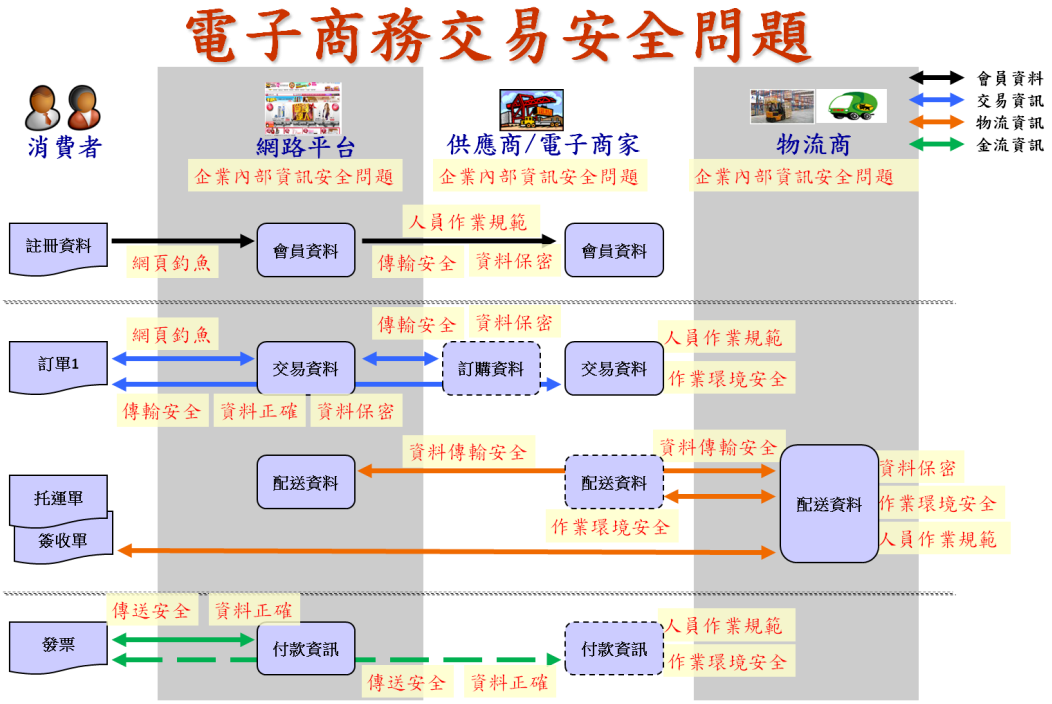
1. 第一類物流商：僅接觸紙本(含印出之配送單、簽收單及手寫快遞單正副本)配送資料之物流商。
2. 第二類物流商：與網路平台、供應商之間，有連線或離線的電子資料交換、傳送等作業流程之物流商，或其本身擁有物流服務網路平台、物流配送作業管理系統等之物流商。

二、規範之文件位階

本規範主要為電子商務產業專用之二階規範暨三階指引。二階規範定義為電子商務業者依據分級所必要遵循或執行之安全作為；規範內容多數係依據相關法令法規與國際標準要求制定。三階指引將提供電子商務業者為強化交易安全與客戶資料保護之進階資安作為參考；規範內容係依據國內外各項資安實作手冊制定，並參考連結至商業司相關資安規範。

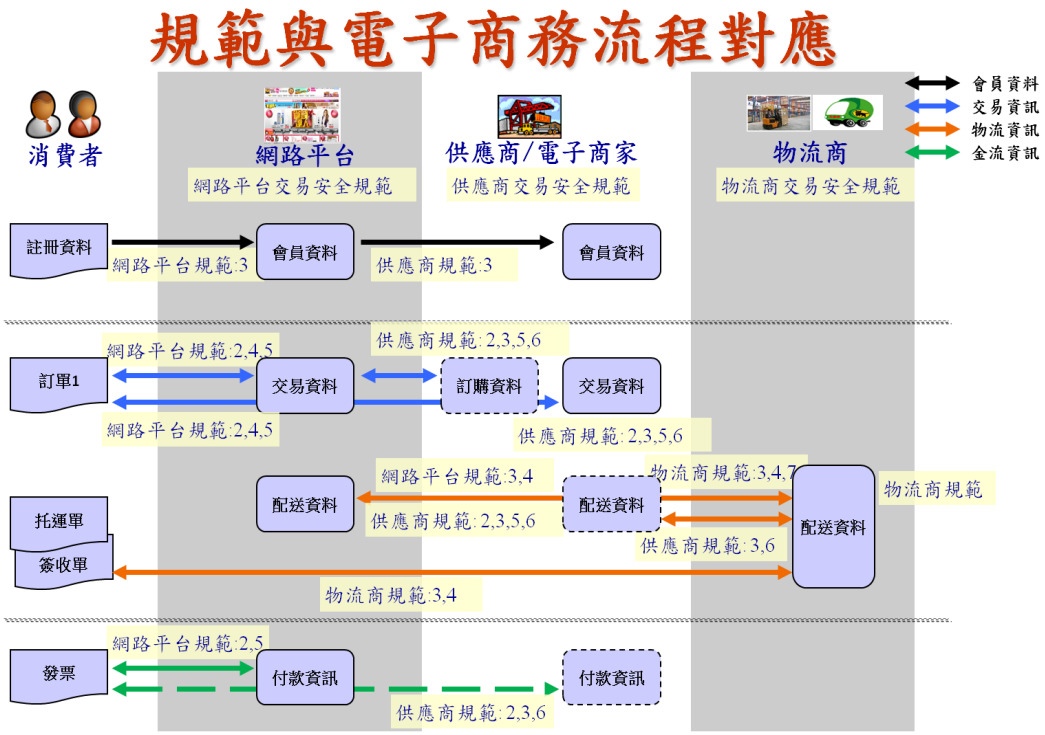
三、規範之實施策略目標

依據規範適用範圍之電子商務業者，所涵蓋之交易服務上下游作業流程，為確保實施 3 份規範能達成之交易安全提升，爰依據上下游作業流程中，應予以保護之重要資訊流(如圖 1、2，表 1)，訂定相對應之實施策略目標。



資料來源：本計畫整理

圖 1　交易服務上下游作業流程重要資訊流與安全問題



資料來源：本計畫整理

圖 2　交易服務上下游作業流程與規範實施策略目標對照

表 1　電子商務交易安全規範實施策略目標

文件名稱	電子商務交易安全規範-網路平台	電子商務交易安全規範-物流商	電子商務交易安全規範-供應商
實施策略目標	1 促進組織資訊安全管理	1.促進組織資訊安全管理	1.促進組織資訊安全管理
	2.加強核心營運系統與資料庫之安全管理	2.加強核心資訊系統安全管理	2.建立營業資訊設備管理
	3.強化客戶個人資料安全管理	3.保護客戶個人資料檔案安全	3.保護客戶個資及作業資料安全
	4.提升企業內資訊環境安全管理	4.建立託運單安全管理	
		5.加強作業環境安全管理	4.加強作業環境安全管理
		6.加強網路安全管理	5.加強網路安全管理
	5.強化對外網站交易平台安全管理	7.建立外部單位資料交換安全管理	6.建立外部單位資料交換安全管理
	6.建立資安通報管理機制	8.建立資安通報管理機制	7.建立資安通報管理機制

資料來源：本計畫整理

四、資訊安全框架

因 ISO 27001/ISO 27002 之資安管理領域架構，為國內與國際最多機構(含電子商務產業)之產業資安標準之參考框架，因此將之列為本規範框架之主要依據。

為補足 ISO 27002 之實作指引對個資管理的深度不足，本規範將另行依據最新之個資法所規範之管理精神，強化電子商務產業客戶個資管理。

五、規範文件結構

(一) 文件結構

為依循電子商務產業特性，以制定管理面、作業面的可達成之原則性的交易安全規範。故將規範文件分為策略目標、規範大綱、要求項目與進階指引共四層之文件結構。

(二) 規範共分為四層

第一層為提升電子商務交易安全之策略目標；

第二層為達成個策略目標之管理項目；

第三層為各管理項目下之具體要求項目；

第四層為達成要求項目之必要或參考查檢表；查檢表之檢核紀錄欄位亦列出於交易安全執行現況中，可作為佐證資訊之相關建議，以提供業者實施本規範之操作面參考。

表 2　規範內容示例

管理項目	要求項目	類別	依據之法規或標準
策略目標：1.促進組織資訊安全管理			
1.2　資訊安全框架	1.1.3 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。	皆適用	ISO 27001
	1.1.4 電子商務網路平台管理階層，應具體說明其對資安之承諾與責任。	皆適用	ISO 27001

資料來源：本計畫整理

(三) 查檢表

1. 為有利於網路平台業者依營運現況進行分類分級實施，並使企業自我檢查或外部第三方查核能有所依據，爰依照各要求

項目制定查檢表。除前述之基本遵守的規範要求以外，特於查檢表中訂定進階指引操作項目，以提供企業參考使用。

2. 查檢表中標示“II”表示僅第二類業者適用。

3. 針對各項規範要求，本規範提供業者必要執行之作業基準查檢項目，及進階查檢項目(進階指引欄位標示◎)。

4. 作業基準查檢項目(Baseline，簡稱 BL)，係為達成各要求項目之交易安全風險基礎管理工作，業者必要且至少應執行之控管作為。

5. 進階查檢項目(Better Practice，簡稱 BP)，係依據各項國際資安實務準則，提供業者參考之進階控管作為，業者得依據資源與風險現況自行決定是否執行。

表 3　查檢表內容示例

編號	要求之查檢項目	類別	進階指引	檢核結果	檢核紀錄
1. 促進組織資訊安全管理					
1.1 資訊安全框架					
1.1.1 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。					
1.1.1.1	是否制定全公司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)？	II		□ 符合 □ 不符合	□ 制定政策，內容包含： - 資訊安全的目標 - 概要資訊安全原則的需求 - 公司內部權責 □ 政策公告內部員工 □ 政策公告給外部廠商 □ 政策定期審查與更新

資料來源：本計畫整理

(四) 附錄

為利於業者對照 ISO 27001、ISO 27002、個人資料保護法以及規範中參考引用之其他管理標準，將規範依查檢項目編號與其對應之法規或標準以及其他可供規範時做參考來源，編列參考文件索引表於附錄中。

另將 3 份規範常見名詞，增列其名詞釋義表於附錄中，但未以所有相關標準出現名詞為涵蓋範圍。

六、未盡事宜

本規範制定時依產業現況與需求，考量文件位階、制定目標、適用範圍及業者實施可能遭遇困難及資源限制，以及目前相關法令法規、產業標準版本發布內容等因素，其有未盡事宜，非為規範之執行限制。已導入相關資訊安全標準之業者，仍建議以符合企業經營及競爭力提升之需求，充分涵括電子商務交易安全相關作業流程或企業整體資訊安全管理流程，施予應有及必要之安全保護，以利電子商務信賴安全環境之發展。

參、規範概述

一、整體大綱

本(供應商)交易安全規範 7 大實施策略目標下，共計 20 個管理項目，僅 14 條為第一類供應商適用之管理項目；37 條要求規範中，僅 16 條為第一類業者適用之應執行之作業基準(Baselines)。規範之下共提供 158 條查檢項目供業者查檢之參考，其中 46 條為第一類業者適用(僅需)查核之項目，其餘 112 條為第二類業者適用查核項目。第二類業者適用查核項目中，亦有 53 條進階指引(Better Practices)之查檢項目，可依據風險管理需求選擇性執行，或依實際執行情形記錄查檢結果。

二、規範導入及 ISO 27001 符合性說明

本(供應商)交易安全規範 7 大實施策略目標與 ISO 27001 管理領域之對照如下，通過 ISO 27001 驗證之業者，可依其資訊安全管理制度適用性聲明文件中，已適用之管理領域與控制項目，對照規範管理項目，以有助於確認規範符合性或強化既有資訊安全管理制度之參考。

表 4　供應商交易安全規範實施範圍

策略目標	管理項目	實施範圍	規範項目數	
			全部	第一類業者適用
1.促進組織資訊安全管理	1.1 資訊安全框架(II) 1.2 資訊資產風險管理(II) 1.3 人力安全管理 1.4 遵循性管理 1.5 客戶及第三方管理(II)	- 管理階層 - 人力資源管理部門(包含委外廠商) - 法律遵循性管理部門(包含智慧財產權、個人資料保護法、消費者保護法等) - 資產風險管理部門	5	2

策略目標	管理項目	實施範圍	規範項目數	
			全部	第一類業者適用
2.建立營業資訊設備管理	2.1 營業資訊設備使用及安全管理 2.2 使用電子商務網路交易平台之存取授權管理	- 負責營業設備或重要核心營運系統維運之管理部門 - 負責系統開發、系統存取控制、機房與作業環境、營運持續等作業流程之執行單位	2	2
3.保護客戶個資及作業資料安全	3.1 客戶個人資料保護 3.2 客戶個資及營業資料之作業安全 3.3 公開交易資訊管理 3.4 配送作業之紙本資料管理	- 涉及客戶個人資料、交易資料、配送資料之作業部門與其作業流程	4	4
4.加強作業環境安全管理	4.1 作業與辦公環境安全管理 4.2 電腦設備環境與設備安全管理 4.3 使用者應遵守安全要求之管理	- 負責公司辦公作業環境管理、資訊作業環境管理之執行單位 - 負責營業用電腦設備管理之執行單位	3	3
5.加強網路安全管理	5.1 網路通訊與資訊作業安全管理(II) 5.2 電子郵件安全管理	- 負責公司整體網路通訊、資訊作業環境管理之執行單位 - 所有使用者	2	1
6.建立外部單位資料交換安全管理	6.1 配送資料電子交換協議與保護(II) 6.2 實體傳遞過程的保護	- 涉及與外部單位進行資料交換之作業單位 - 提供或支援與外部單位資料交換設備之作業單位	2	1
7.建立資安通報管理機制	7.1 電子商務資安事件通報機制 7.2 資安事故管理(II)	- 管理階層 - 負責資訊安全事故管理執行單位	2	1
		小計	20	14

資料來源：本計畫整理

表 5　供應商交易安全規範與 ISO 27001 符合性對照

策略目標	管理項目	ISO 27001 管理領域對照
1.促進組織資訊安全管理	1.1 資訊安全框架(II) 1.2 資訊資產風險管理(II) 1.3 人力安全管理 1.4 遵循性管理 1.5 客戶及第三方管理(II)	- 本文(4.2, 4.3,6) - 組織管理(A.6) - 資產管理(A.7) - 人員安全管理(A.8) - 通訊與作業管理(A.10) - 遵循性管理(A.15)
2.建立營業資訊設備管理	2.1 營業資訊設備使用及安全管理 2.2 使用電子商務網路交易平台之存取授權管理	- 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12)
3.保護客戶個資及作業資料安全	3.1 客戶個人資料保護 3.2 客戶個資及營業資料之作業安全 3.3 公開交易資訊管理 3.4 配送作業之紙本資料管理	- 人員安全管理(A.8) - 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 遵循性管理(A.15)
4.加強作業環境安全管理	4.1 作業與辦公環境安全管理 4.2 電腦設備環境與設備安全管理 4.3 使用者應遵守安全要求之管理	- 人員安全管理(A.8) - 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 資訊安全事故管理(A.13) - 遵循性管理(A.15)
5.加強網路安全管理	5.1 網路通訊與資訊作業安全管理(II) 5.2 電子郵件安全管理	- 通信與作業管理(A.10) - 存取控制管理(A.11) - 遵循性管理(A.15)
6.建立外部單位資料交換安全管理	6.1 配送資料電子交換協議與保護(II) 6.2 實體傳遞過程的保護	- 通信與作業管理(A.10) - 資訊系統開發及維護管理(A.12)
7.建立資安通報管理機制	7.1 電子商務資安事件通報機制 7.2 資安事故管理(II)	- 資訊安全事故管理(A.13)

資料來源：本計畫整理

肆、規範內容

說明：

本節為本規範要求項目所有內容，其表列順序依照第參章第一節整體大綱，內容涵括規範之第一層至第三層，並標示每一條規範之適用業者分類類別以及依據之法規或標準名稱。

表 6　供應商交易安全規範要求項目表

管理項目	要求項目	類別	依據之法規或標準
策略目標：1. 促進組織資訊安全管理			
1.1 資訊安全框架	1.1.1 供應商之管理階層，應具體說明其對資安之承諾與責任。	II	ISO 27001
1.2 資訊資產風險管理	1.2.1 供應商應說明目前持有之客戶個資擋案範圍，及其保護之方法。	II	ISO 27001
1.3 人力安全管理	1.3.1 應對相關作業人員進行資安教育訓練與宣導，內容至少包含客戶資料管理相關法規與本規範所涉之內容，並於離職或職務變更時移除或修改權限。		ISO 27001
1.4 遵循性管理	1.4.1 電子商務營業應遵守民法、刑法、消保法、公平交易法、智慧財產權與個資法等相關法令法規，並滿足所提供之服務契約要求。		ISO 27001
1.5 客戶及第三方管理	1.5.1 選擇商業夥伴(包含供應商、賣方廠商、運輸業者、倉儲服務、定點取件服務、金流服務或資訊服務廠商)時，應充分考量其資安能力與配合度。	II	ISO 27001
策略目標：2. 加強營業資訊設備管理			
2.1 營業資訊設備使用及安全管理	2.1.1 營業用電腦設備應安裝防毒軟體，並定期更新病毒碼及執行系統掃描作業。		ISO 27001
	2.1.2 應定期進行營業應用系統之資訊、軟體與系統的備份與還原測試，並確保備份資料儲存場所的安全。	II	ISO 27001
	2.1.3 所有交易相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。	II	ISO 27001
2.2 使用電子商務網路交易平台之存取授權管理	2.2.1 應管制電子商務網路平台提供之操作帳號與密碼，以保護消費者資料與交易資訊。		ISO 27001
	2.2.2 若有委外開發、租賃或自有之電子商務營運相關資訊系統，採用前應有相關安全要求，使用及維護應有相關安全管理規定。	II	ISO 27001
策略目標：3. 保護客戶個資及營業資料安全			

管理項目	要求項目	類別	依據之法規或標準
3.1 客戶個人資料保護	3.1.1 應成立管理組織並依作業需求指定作業人員之權責，以依相關法令辦理安全維護及客戶個人資料保管事項。		ISO 27001、「個人資料保護法」
	3.1.2 宜依實際作業流程，制定客戶資料蒐集、處理、利用，與當事人可行使權利之程序。		ISO 27001、「個人資料保護法」
3.2 客戶個資及營業資料之作業安全	3.2.1 應保護紙本或電子形式的客戶個人資料、交易資料以及物流配送資料，並於使用目的結束後予以銷毀或刪除。		ISO 27001、「個人資料保護法」
	3.2.2 欲廢棄或不再持有之大量內含客戶資訊之紙本資料應確實銷毀，或委由專業處理廠商於專人監督下銷毀。	II	ISO 27001、「個人資料保護法」
3.3 公開交易資訊管理	3.3.1 應遵循「零售業等網路交易定型化契約應記載及不得記載事項」之法令規定，並維護網站公告資訊之正確性。		「消費者保護法」、ISO 27001
3.4 配送作業之紙本資料管理	3.4.1 客戶託運單、快遞郵寄包裝外顯示之配送資訊，應避免出現完整之客戶個人資料，並對託運紙本資料進行保護。		ISO 27001、「個人資料保護法」
	3.4.2 托運單資料應於安全處所妥為保管，並於安全之實體環境中進行列印。	II	ISO 27001
策略目標：4. 加強作業環境安全管理			
4.1 作業與辦公環境安全管理	4.1.1 應確保作業與辦公場所之安全，避免火災、竊盜或惡意破壞等損害。		ISO 27001
	4.1.2 應對進出作業與辦公場所、託運單、出貨單儲存及電腦設備機房等區域進行身份確認，並監控其作業行為。	II	ISO 27001
4.2 電腦設備環境與設備安全管理	4.2.1 設備外送或淘汰時應防止資訊外洩。		ISO 27001
	4.2.2 應設計安全措施，確保營業用電腦伺服器與網路設備之安全，避免遭到竊盜或損害。	II	ISO 27001
	4.2.3 應制定使用者電腦使用管理規範，對使用者電腦使用、資訊設備管理之安全規範。	II	ISO 27001
4.3 使用者應遵守安全要求之管理	4.3.1 應配合電腦使用安全規定，如設定並定期更新登入密碼、系統更新，以及電腦使用、資訊設備操作、遵守上網之安全性等需注意事項。		ISO 27001
策略目標：5. 加強網路安全管理			

管理項目	要求項目	類別	依據之法規或標準
5.1 網路通訊與資訊作業安全管理	5.1.1 任何對於客戶資料之查調、處理等作業，應於可滿足業務需求與合理人力分工之前提下，採用最小揭露與最小權限原則。	II	ISO 27001
	5.1.2 應對無線網路之使用進行規定並限制外來使用。	II	ISO 27001
	5.1.3 宜對公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，有相關的網站伺服器強化措施及定期執行網站技術弱點處理程序。	II	ISO 27001
5.2 電子郵件安全管理	5.2.1 應對電子郵件程式進行相關安全設定，如需傳送客戶資料或訂單資料宜加密保護。		ISO 27001
	5.2.2 應定期對執行電子商務作業之電子郵件帳號進行密碼變更要求。		ISO 27001
	5.2.3 應制定電子郵件使用規則，並對人員進行郵件使用宣導，以維護使用郵件的系統與應用程式的安全。	II	ISO 27001
	5.2.4 應設置防止垃圾郵件或設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件。	II	ISO 27001
策略目標：6. 建立外部單位資料交換安全管理			
6.1 配送資料電子交換協議與保護	6.1.1 應與電子商務網路平台(含平台商、物流商)及涉入電子商務交易流程之商業合作夥伴，協定各作業流程之電子資料交換機制(含資料往返、互換及二次以上傳遞)，並予以保護。	II	ISO 27001
	6.1.2 宜限制高風險業務或敏感性資訊避免使用即時通訊軟體或外部電子郵件信箱進行資料傳輸作業。	II	ISO 27001
6.2 實體傳遞過程的保護	6.2.1 應保護內有客戶資料之儲存媒體(如磁片、光碟片及磁帶)，連同消費者之貨品交寄皆應採用可靠之遞送管道並取得收訖證明。		ISO 27001
策略目標：7. 建立資安事件通報管理機制			
7.1 電子商務資安事件通報機制	7.1.1 應建立「電子商務資安事件通報機制規範」通報方式之認知。		ISO 27001
	7.1.2 應參照「電子商務資安事件通報機制規範」，進行資安事故外部通報。	II	ISO 27001
7.2 資安事故管理	7.2.1 應建立內部資安事件通報程序，並對內外部員工宣導相關通報流程。	II	ISO 27001
	7.2.2 應收集、保存及呈現資安事故之完整證據，並針對事故之原因進行檢討分析。	II	ISO 27001

資料來源：本計畫整理

伍、規範查檢表

說明：

(一) 查檢表格式依循規範大綱及管理項目，分別制定要求之查檢項目與對應之檢核方法

(二) 類別欄位標示“皆適用”者，表示第 1、2 類業者皆適用；標示“II”表示僅第 2 類業者適用。

(三) 進階指引欄位標示“◎”表示為進階指引(Better Practices)之參考項目，可依據風險管理需求選擇性執行；未標示者表示該查檢項目為應執行之作業基準(Baselines)，業者應落實執行。

(四) 檢核結果欄位，提供業者自我查核或第三方查核時，針對該查檢項目之查核結果，記錄執行現況是否符合要求。進階指引項目於查核前，應先辨識該項目是否適用，經辨識為不適用項目者，毋須再做檢核紀錄。

(五) 檢核紀錄欄位，提供業者自我查核或第三方查核時，針對該查檢項目之執行現況予以記錄。該欄位已列出之相關紀錄確認，為提供業者實施本規範之操作面參考，非為執行限制，故檢核紀錄可增列所有實際檢核之佐證資訊。

表 7　規範查檢表

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1. 促進組織資訊安全管理					
1.1 資訊安全框架					
1.1.1	供應商之管理階層，應具體說明其對資安之承諾與責任。				

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.1.1.1	管理階層是否制定基本的資安須知，並告知全體員工與委外廠商予以落實？	II		☐ 適用 ☐ 不適用 說明：	☐ 制定資安須知，內容包含： - 資訊安全目標 - 組織內部權責 - 基本資安守則 ☐ 政策公告內部員工 ☐ 政策公告給外部廠商
1.1.1.2	是否指定專人，負責辦理資安須知、計畫、守則之研議，電子商務網路平台系統之使用管理及保護，資安認知教育訓練，等資訊安全範圍內之工作事項？	II		☐ 適用 ☐ 不適用 說明：	
1.2 資訊資產風險管理					
1.2.1 供應商應說明目前持有之客戶個資檔案範圍，及其保護之方法。					
1.2.1.1	若達第二類業者規模，是否參考「電子商務交易安全規範-網路平台：1.3 資訊資產管理」考量適當查檢項目予以落實？	II		☐ 適用 ☐ 不適用 說明：	
1.2.1.2	若達第二類業者規模，是否已依據「電子商務交易安全規範-網路平台：1.2 風險管理」考量適當查檢項目予以落實？	II		☐ 適用 ☐ 不適用 說明：	
1.2.1.3	若達第二類業者規模，是否參考「電子商務交易安全規範-網路平台：2.5 核心營運系統營運持續管理」考量適當查檢項目予以落實？	II	◎	☐ 適用 ☐ 不適用 說明：	
1.3 人力安全管理					
1.3.1 應對相關作業人員進行資安教育訓練與宣導，內容至少包含客戶資料管理相關法規與本規範所涉之內容，並於離職或職務變更時移除或修改權限。					
1.3.1.1	電子商務相關作業人員(包含可接觸相關資訊或作業地點)是否皆瞭解保密事項並簽署保密協議？			☐ 適用 ☐ 不適用 說明：	
1.3.1.2	是否對電子商務相關作業人員(包含可接觸相關資訊或作業地點)提供資訊安全、客戶資料保護、電腦使用守則等認知教育訓練？			☐ 適用 ☐ 不適用 說明：	☐ 施行資安教育訓練並留存訓練紀錄 ☐ 施行客戶隱私保護相關教育訓練與規定

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					□ 內部員工參與
1.3.1.3	電子商務相關作業人員(含約聘僱員工或外部合約廠商)於離職或合約終止時，時，是否依規定繳回其使用或保管之電腦資產(包含歸還所有先前發出的軟體、文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有公司資產)？			□ 適用 □ 不適用 說明：	
1.3.1.4	電子商務相關作業人員(含約聘僱員工或外部合約廠商)，在其聘僱合約、契約或協議變更調整或終止時，是否將其內部資訊系統與電子商務網路平台之相關存取權限予以移除？			□ 適用 □ 不適用 說明：	
1.4 遵循性管理					
1.4.1 電子商務營業應遵守民法、刑法、消保法、公平交易法、智慧財產權與個資法等相關法令法規，並滿足所提供之服務契約要求。					
1.4.1.1	是否確保均不違反任何法律、法令、法規或契約義務，以及任何安全要求？			□ 適用 □ 不適用 說明：	
1.4.1.2	物流商是否參考「電子商務交易安全規範-網路平台:1.5 遵循性管理」予以落實查檢項目？			□ 適用 □ 不適用 說明：	
1.5 客戶及第三方管理					
1.5.1 選擇商業夥伴(包含供應商、賣方廠商、運輸業者、倉儲服務、定點取件服務、金流服務或資訊服務廠商)時，應充分考量其資安能力與配合度。					
1.5.1.1	基於供應鏈安全之考量，選擇電子商務交易相關之商業夥伴，包含供應商、賣方廠商、倉儲服務、運輸業者、定點取件服務、金流服務或資訊服務廠商等，是否具有書面且可供驗證之程序？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.2	選擇服務供應商前，是否進行服務供應商之資訊安全風險評估程序？(例如要求檢視其資訊安全 ISO 27001 之認證影本，以證明該商業夥伴已取得資訊安全認證。)	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.5.1.3	未具資訊安全認證之商業夥伴是否備有如下符合資訊安全基準要求之書面證明文件？ 1. 要求未具資訊安全認證之商業夥伴提供下列其中一項遵守資訊安全基準之書面證明： (1) 契約文件。 (2) 提供一份申請人交填之資訊安全審查項目及驗證基準自我評估表。 (3) 商業夥伴書面聲明其符合資訊安全基準要求。 (4) 商業夥伴之高層人員簽署保證符合資訊安全基準要求之信函。 2. 未具資訊安全資格之商業夥伴無法提供書面證明時，申請人須依據書面之風險評估程序確認其符合資訊安全基準。	II	◎	☐ 適用 ☐ 不適用 說明：	
1.5.1.4	金流服務供應商是否已通過具有公信力之 PDCA 資訊安全管理制度驗證，且驗證範圍包含其產品之資訊處理流程，如：ISO 27001 或 PCI-DSS？	II	◎	☐ 適用 ☐ 不適用 說明：	
1.5.1.5	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。	II		☐ 適用 ☐ 不適用 說明：	☐ 針對服務供應商進行評估並留存書面紀錄
1.5.1.6	與觸及合約資訊、營業資料及客戶交易資料之委外服務供應商簽訂合約時，內容是否至少包含但不限於下列精神之保密敘述： (1) 對於公司之客戶資料負絕對之保密義務及保管責任，未經本公司同意，絕不以任何方式將其洩露、告知、交付予任何第三人，若有違反以致公司遭受損害，合約廠商應同意無條件賠償本公司所受之一切	II		☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	損害(包括訴訟上及非訴訟上之損害)。 (2) 另如涉有民刑事責任，合約廠商並應負起相關所有民刑事責任。				
1.5.1.7	觸及合約資訊、營業資料及客戶交易資料之服務供應商，其處理人員是否簽訂保密切結書？	II		□ 適用 □ 不適用 說明：	□ 處理人員簽訂保密切結
1.5.1.8	委外廠商之資訊安全聲明中是否包含應瞭解並確實遵守政府、主管機關等之相關資訊安全法令規定，若有違反願配合公司進行調查？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.9	若委外廠商將與公司有關之作業委外，是否以書面方式知會？是否對轉包單位、人員、資訊實施必要之管制與監控？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.10	若委外廠商或其委外廠商發生資安事件導致客戶資料外洩者，服務供應商是否以書面聲明願負起完全連帶擔保責任？	II		□ 適用 □ 不適用 說明：	
1.5.1.11	是否與電子商務網路平台或第三方資訊委外服務廠商簽訂適當服務定義及交付等級，並賦予相關的安全管理責任，且納入契約條款？	II	◎	□ 適用 □ 不適用 說明：	□ 與外部廠商簽訂服務等級協定 □ 與外部廠商簽訂安全管理責任
1.5.1.12	由委外廠商或合作廠商等第三方提供之服務如有任何異動時，是否評估資安措施之有效性並作必要之調整？	II	◎	□ 適用 □ 不適用 說明：	
2. 加強營業資訊設備管理					
2.1 營業資訊設備使用及安全管理					
2.1.1 營業用電腦設備應安裝防毒軟體，並定期更新病毒碼及執行系統掃描作業。					
2.1.1.1	是否至少每月進行對營業用作業電腦與其相關資料儲存媒體進行病毒與後門程式之完整系統掃描？			□ 適用 □ 不適用 說明：	
2.1.1.2	電腦內是否安裝合法防毒軟體，並設定自動更新(或至少每天一次)病毒碼與掃描引擎？			□ 適用 □ 不適用 說明：	□ 安裝防毒軟體 □ 每日更新
2.1.2 應定期進行營業應用系統之資訊、軟體與系統的備份與還原測試，並確保備份資料儲存場所的安全。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1.2.1	是否每週針對營業用資訊系統與軟體進行備份？	II		□ 適用 □ 不適用 說明：	
2.1.2.2	是否每日備份正在處理中之客戶交易資料？	II		□ 適用 □ 不適用 說明：	□ 每日備份檔案
2.1.2.3	是否考量每月備份、統一管理、或銷毀/刪除交易完成之客戶往來資料？	II		□ 適用 □ 不適用 說明：	
2.1.2.4	備份是否儲存於遠端地點？距離是否足以避免機房與辦公主要場地發生災難時遭波及？	II	◎	□ 適用 □ 不適用 說明：	
2.1.2.5	備份資訊是否給予適切等級的實體與環境保護，並與機房與及主要辦公作業地點使用的標準一致？(機房與辦公主要場地採用的控制措施，可延伸至備份作業場地)	II	◎	□ 適用 □ 不適用 說明：	
2.1.3 所有交易相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。					
2.1.3.1	所有系統或監視錄影之日期與時間設定是否每週核對校正以確保時間記錄正確？	II		□ 適用 □ 不適用 說明：	□ 時間誤差不超過三分鐘
2.2 使用電子商務網路交易平台之存取授權管理					
2.2.1 應管制電子商務網路平台提供之操作帳號與密碼，以保護消費者資料與交易資訊。					
2.2.1.1	使用電子商務網路平台或與平台界接之相關營業系統，是否採用使用者權限申請表單進行存取權限之核准？			□ 適用 □ 不適用 說明：	
2.2.1.2	使用電子商務網路平台或與平台界接之相關營業系統，若使用者變更權責、調職或離職，是否立即移除或停用其權限？			□ 適用 □ 不適用 說明：	
2.2.1.3	是否立即更新電子商務網路平台業者發放之預設使用者密碼？			□ 適用 □ 不適用 說明：	
2.2.1.4	使用電子商務網路平台系統或與平台界接之相關營業系統，使用者密碼是否每三個月定期更改？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.2.1.5	員工使用電子商務網路平台系統或與平台界接之相關營業系統，是否採用單一可識別個人的帳號與密碼？若平台僅配發一定數量之帳號或實際作業所需，是否列出使用清單並由管理人員循檢			□ 適用 □ 不適用 說明：	
2.2.2 若有委外開發、租賃或自有之電子商務營運相關資訊系統，採用前應有相關安全要求，使用及維護應有相關安全管理規定。					
2.2.2.1	若達第二類業者規模，是否參考「電子商務交易安全規範-網路平台：2.1 核心營運系統取得、開發及維護安全管理」考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
3. 保護客戶個資及營業資料安全					
3.1 客戶個人資料保護					
3.1.1 應成立管理組織並依作業需求指定作業人員之權責，以保護客戶個人資料之安全，並確保個人資料之公布取得依據或授權。					
3.1.1.1	是否指定專人依相關法令辦理客戶個人資料安全維護與保管事項？			□ 適用 □ 不適用 說明：	
3.1.1.2	是否能防止在內外部網站或網頁，在沒有取得客戶同意及主管授權或有法律依據、合約等情況下公布客戶個人資料？			□ 適用 □ 不適用 說明：	
3.1.2 宜依實際作業流程，制定客戶資料蒐集、處理、利用，與當事人可行使權利之程序。					
3.1.2.1	客戶資料之蒐集、處理、利用，與當事人可行使權利是否有實際作業流程管理程序，明文制定並公告客戶必要知悉之資訊？			□ 適用 □ 不適用 說明：	
3.2 客戶個資及營業資料之作業安全					
3.2.1 應保護紙本或電子形式的客戶個人資料、交易資料以及物流配送資料，並於使用目的結束後予以銷毀或刪除。					
3.2.1.1	作業環境之電腦，若留存一週以上且非日常業務頻繁使用之客戶資料檔案、交易資料以及物流配送資料，是否以密碼加密？			□ 適用 □ 不適用 說明：	
3.2.1.2	作業環境之電腦，是否不儲存業務目的消失後超過一週以上之客戶資料檔案、交易資料以及物流配送資料？			□ 適用 □ 不適用 說明：	□ 留有備份

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.2.1.3	作業環境之電腦，是否未安裝 P2P 點對點分享軟體，避免資料外洩？			□ 適用 □ 不適用 說明：	
3.2.1.4	是否每週備份營業電腦設備中客戶資料檔案、交易資料以及物流配送資料？	II		□ 適用 □ 不適用 說明：	
3.2.1.5	客戶資料、交易資料、物流配送資料，是否集中控管於權限控管之公用資料夾，並依業務需求定期刪除？	II	◎	□ 適用 □ 不適用 說明：	
3.2.1.6	客戶資料與物流配送資料是否每月備份為光碟存檔，並由專人上鎖保管？	II	◎	□ 適用 □ 不適用 說明：	
3.2.1.7	是否每日檢查環境周遭是否有列印出的客戶資料、交易資料以及物流配送資料，若有則一律銷毀？			□ 適用 □ 不適用 說明：	
3.2.1.8	授權處理機敏資料作業相關人員於作業中離開座位或下班時，是否妥善收存書面形式之機敏資料？			□ 適用 □ 不適用 說明：	
3.2.1.9	傳真設備是否有周期循檢，以確保傳真進件之機敏資料妥善置於處理人員作業區域？			□ 適用 □ 不適用 說明：	
3.2.1.10	無須歸檔的紙本文件資料內若有機敏資料，是否於使用完畢後使用碎紙機銷毀？			□ 適用 □ 不適用 說明：	
3.2.1.11	各項電子形式之資料報表，是否於完成處理作業後，每季定期進行檔案之刪除作業？	II		□ 適用 □ 不適用 說明：	
3.2.1.12	公司是否依循電子商務網路平台業者業者所建立之客戶資料保護管理架構、指引或建議機制，予以落實？	II		□ 適用 □ 不適用 說明：	
3.2.1.13	若達第二類業者規模，是否參考「電子商務交易安全規範-網路平台：3強化客戶個人資料管理 」考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
3.2.2 欲廢棄或不再持有之大量內含客戶資訊之紙本資料應確實銷毀，或委由專業處理廠商於專人監督下銷毀。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.2.2.1	內含客戶資訊之紙本資料，其保存年限屆滿或業務目的消失時，是否有相關之程序主動銷毀？	II		□ 適用 □ 不適用 說明：	
3.2.2.2	客戶個人資料銷毀承辦人員是否向部門主管提出申請核備？於核可後方得辦理銷毀。	II	◎	□ 適用 □ 不適用 說明：	
3.2.2.3	大量之客戶資料檔案文件銷毀是否統一分配裝箱並黏貼封條？	II		□ 適用 □ 不適用 說明：	
3.2.2.4	紙本資料銷毀方式是否採用水銷處理法、焚毀等確實銷毀之方法？	II		□ 適用 □ 不適用 說明：	
3.2.2.5	由委外廠商協助銷毀時，是否指派監督人員跟隨，並予以拍照並在其監督下進行銷毀？	II		□ 適用 □ 不適用 說明：	
3.2.2.6	銷毀過程中是否全程錄影且監控整個作業流程，以確保無任何個資外洩之可能性？	II	◎	□ 適用 □ 不適用 說明：	
3.2.2.7	是否保留銷毀作業之收件紀錄及銷毀場之銷毀證明至少 N(N>=1)年存查？	II	◎	□ 適用 □ 不適用 說明：	
3.3 公開交易資訊管理					
3.3.1 應遵循「零售業等網路交易定型化契約應記載及不得記載事項」之法令規定，並維護網站公告資訊之正確性。					
3.3.3.1	是否由每日審查確認網站之公告訊息與商品資訊之正確性？			□ 適用 □ 不適用 說明：	
3.3.3.2	是否建立價格或下單交易大量或異常之預警機制？	II	◎	□ 適用 □ 不適用 說明：	□ 考量設定商品下單數量之上限 □ 考量電子提醒方式建立異常預警
3.4 配送作業之紙本資料管理					
3.4.1 客戶託運單、快遞郵寄包裝外顯示之配送資訊，應避免出現完整之客戶資訊，並對託運紙本資料進行保護。					
3.4.1.1	除配送或揀貨等實務作業之必要資訊外，客戶託運單、快遞郵寄包裝外所顯示之相關資訊是否盡量予以			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	適當遮隱？且是否避免出現客戶身分証號、各種金流交易資訊及發票等隱私或敏感資料？				
3.4.1.2	託運單處理作業相關人員於作業中離開座位或下班時，是否妥善收存紙本託運單並鎖定電腦避免處理中之託運資料外洩？			□ 適用 □ 不適用 說明：	
3.4.1.3	是否每日檢查作業環境周遭是否有未妥善保管之託運單？			□ 適用 □ 不適用 說明：	
3.4.1.4	當週需應用於查詢之紙本託運單，是否集中於上鎖鐵櫃，並由專人控管鑰匙？	II		□ 適用 □ 不適用 說明：	
3.4.1.5	當週紙本託運單之調閱是否僅限現場作業之授權人員？	II		□ 適用 □ 不適用 說明：	
3.4.2 托運單資料應於安全處所妥為保管，並於安全之實體環境中進行列印。					
3.4.2.1	是否將留存一週以上之紙本託運單集中保管？	II		□ 適用 □ 不適用 說明：	
3.4.2.2	託運單之調閱是否填寫託運單紙本調閱申請表方得調閱？	II	◎	□ 適用 □ 不適用 說明：	
3.4.2.3	託運單紙本調閱表單是否由專人控管借出與交回，且需於託運單交回後再行簽章確認？	II	◎	□ 適用 □ 不適用 說明：	
3.4.2.4	客服部門等相關定期調閱單位是否每日以報表控管調閱單據，且經主管核章後歸檔？	II	◎	□ 適用 □ 不適用 說明：	
3.4.2.5	是否指定專人限制於特定電腦才可進行宅配單列印作業？	II		□ 適用 □ 不適用 說明：	
3.4.2.6	託運單列印電腦是否與網際網路隔離？	II		□ 適用 □ 不適用 說明：	
3.4.2.7	是否將當日託運單檔案自列印電腦中刪除？	II		□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4. 加強作業環境安全管理					
4.1 作業與辦公環境安全管理					
4.1.1 應確保作業與辦公場所之安全，避免火災、竊盜或惡意破壞等損害。					
4.1.1.1	是否對於處理電子商務作業之辦公場所、出貨倉庫、電腦設備機房等相關重要場所劃分管制區域，並於出入口設置門鎖、門禁或保全連線等安全措施？			□ 適用 □ 不適用 說明：	
4.1.1.2	管制區域內外窗戶、圍籬或大門是否以可上鎖或以其他符合安全之替代方法加以管理，並由管理或保全人員控管鑰匙之領用？			□ 適用 □ 不適用 說明：	
4.1.1.3	電子商務相關作業員工是否易於辨識身份(如：配戴識別證或穿著制服或採用進出登記、門禁管制等)以保護？			□ 適用 □ 不適用 說明：	
4.1.1.4	電子商務作業區域是否裝置適當消防設施，或於人員可及之範圍內置放滅火器或消防設備？			□ 適用 □ 不適用 說明：	□有滅火器 □有保全消防裝置 □有火警偵測或自動滅火裝置
4.1.2 應對進出作業與辦公場所、託運單、出貨單儲存及電腦設備機房等區域進行身份確認，並監控其作業行為。					
4.1.2.1	是否配置員工或外聘保全公司負責管制區域之保全工作？	II		□ 適用 □ 不適用 說明：	
4.1.2.2	是否訂有核發、收回及更換進出裝置(例如：鑰匙、門禁卡等)之程序及文件紀錄？	II	◎	□ 適用 □ 不適用 說明：	
4.1.2.3	是否建置適當管控員工識別證之核發及收回機制？	II		□ 適用 □ 不適用 說明：	
4.1.2.4	訪客或委外廠商進出管制區域是否需進行登記並由接洽人員陪同進出，並佩戴明顯之臨時識別證？	II		□ 適用 □ 不適用 說明：	
4.1.2.5	是否針對電腦機房、重要文件存放庫房等管制區域裝設監視錄影設備，並保留一週以上的錄影紀錄？	II		□ 適用 □ 不適用 說明：	□ 備有監視錄影設備 □ 存有一週以上之錄影紀錄

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.1.2.6	是否利用警報系統或監視錄影設備監控處理託運資料相關之重要出入口，防止未經許可人員進出貨物處理及倉儲區域，避免未經許可人員接觸貨物上之客戶資訊及電腦設備？	II		□ 適用 □ 不適用 說明：	□ 備有監視錄影設備 □ 存有一週以上之錄影紀錄
4.1.2.7	是否對於未經授權進入管制區域及非法侵入事件須訂有通報之程序？	II	◎	□ 適用 □ 不適用 說明：	
4.1.2.8	作業用電腦設備是否訂有保護措施，如：使用授權管理、設通行密碼、檔案加密、專人看管？	II		□ 適用 □ 不適用 說明：	
4.1.2.9	無人看管之營業用電腦或網路設備(如：網路集線器)是否上鎖並定期檢查？	II		□ 適用 □ 不適用 說明：	□ 予以上鎖 □ 定期檢查
4.2 電腦設備環境與設備安全管理					
4.2.1 設備外送或淘汰時應防止資訊外洩。					
4.2.1.1	相關電腦設備或儲存媒體異動或遞送時，是否定有相關的程序進行管理？	II	◎	□ 適用 □ 不適用 說明：	□ 移除版權軟體 □ 進行格式化
4.2.1.2	人員攜帶電腦設備與媒體進出管制區域時，是否記錄於表單？	II		□ 適用 □ 不適用 說明：	
4.2.1.3	更新、維修或報廢電腦設備時，是否備份並刪除其中儲存之客戶資料檔案、交易資料以及物流配送資料？若對外送修時，是否選擇信賴商家或先行取出硬碟？			□ 適用 □ 不適用 說明：	
4.2.1.4	電腦設備送修時，若非屬儲存媒體(如：硬碟)損壞，於送修前是否先取出儲存媒體，不得一起送修？	II		□ 適用 □ 不適用 說明：	
4.2.1.5	儲存媒體送修時，若內含客戶資料或機敏資訊時，是否先進行備份，存放於安全區域，並刪除送修設備上之資料防止外洩？	II		□ 適用 □ 不適用 說明：	
4.2.1.6	硬體類設備報廢時，是否由保管單位刪除或格式化所報廢設備內之資料？	II		□ 適用 □ 不適用 說明：	
4.2.2 應設計安全措施，確保營業用電腦伺服器與網路設備之安全，避免遭到竊盜或損害。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.2.2.1	置放電腦伺服器與網路設備置之機房，是否僅限受允許之員工進出？	II		□ 適用 □ 不適用 說明：	
4.2.2.2	電腦伺服器與網路設備是否置放於機櫃或桌上？	II		□ 適用 □ 不適用 說明：	
4.2.2.3	通信纜線(communications cables)及電源纜線是否隔離，以防止互相干擾？	II	◎	□ 適用 □ 不適用 說明：	
4.2.2.4	是否備有溫、濕度計，定時登記監控溫度與濕度？	II		□ 適用 □ 不適用 說明：	
4.2.2.5	營業用電腦伺服器系統等關鍵設施是否備有 UPS 不斷電系統？	II		□ 適用 □ 不適用 說明：	
4.2.2.6	備援電源(如：發電機)是否定期檢查並測試，確保能在斷電期間運作？	II	◎	□ 適用 □ 不適用 說明：	
4.2.2.7	設備之維護與修理是否僅由授權之維護人員執行？	II		□ 適用 □ 不適用 說明：	
4.2.2.8	如採自建機房維運核心營運系統或建置於委外機房，是否參考「電子商務交易安全規範-網路平台：2.3.核心營運系統機房與作業環境實體安全」考量適當查檢項目進行落實？	II	◎	□ 適用 □ 不適用 說明：	
4.2.3 應制定使用者電腦使用管理規範，對使用者電腦使用、資訊設備管理之安全規範。					
4.2.3.1	機房用機、值班用機或是程式執行之限制需常態開機之電腦，是否定期重新開機，以利開機時完成相關修補程式及病毒碼之更新作業，同時避免電腦遭未經授權的存取？	II	◎	□ 適用 □ 不適用 說明：	
4.2.3.2	是否考量資料安全性，針對桌上型電腦的 USB 連接埠停用大量儲存媒體裝置與軟碟機之使用功能？並建立管制與申請程序。	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.2.3.3	公司內部與網際網路連線之個人電腦(含移動式電腦)，是否未儲存非即時作業所需之客戶相關交易資料？	II	◎	□ 適用 □ 不適用 說明：	
4.2.3.4	是否定有適當之控制措施，以防止影印機和其他重製技術(例如：掃描器、數位相機)的未經授權使用？	II	◎	□ 適用 □ 不適用 說明：	
4.2.3.5	是否考量限制將未經授權允許之資訊設備、軟硬體攜入辦公場所使用？	II	◎	□ 適用 □ 不適用 說明：	
4.2.3.6	非公司配發及採購之週邊設備，是否考量禁止擅自安裝於內部電腦上？	II	◎	□ 適用 □ 不適用 說明：	
4.2.3.7	是否建立一般同仁公司配發之電腦遺失或遺失之通報流程與報案、資產風險控管程序？	II	◎	□ 適用 □ 不適用 說明：	
4.3 使用者應遵守安全要求之管理					
4.3.1 應配合電腦使用安全規定，如設定並定期更新登入密碼、系統更新，以及電腦使用、資訊設備操作、遵守上網之安全性等需注意事項。					
4.3.1.1	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？			□ 適用 □ 不適用 說明：	□ 作業系統更新是否一致 □ 更新時程≦1個月
4.3.1.2	執行電子商務營運之個人電腦(含移動式電腦)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？			□ 適用 □ 不適用 說明：	
4.3.1.3	下班時是否登出電腦系統並關閉電源？			□ 適用 □ 不適用 說明：	
4.3.1.5	包含敏感或機密資訊的文件是否立即從印表機或傳真機上取走？			□ 適用 □ 不適用 說明：	
4.3.1.6	是否設定作業系統內建之螢幕保護程式，以確保公司資料之安全性？			□ 適用 □ 不適用 說明：	□ 螢幕保護程式設定≦5 分鐘並以密碼保護
4.3.1.7	下班後經辦之機密性及敏感性資訊或文件是否妥為收存？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.3.1.8	是否限制瀏覽高風險網站，並避免透過Web方式傳送機密業務資料及敏感性資料？	II		□ 適用 □ 不適用 說明：	
4.3.1.9	是否經由資訊單位或管理權責單位定期審查 Internet 內容瀏覽限制、網站過濾規則性？	II	◎	□ 適用 □ 不適用 說明：	
4.3.1.10	是否有監控網站或過濾網站之運作機制？若有系統或流量異常狀況，應以電話或電子郵件方式告知管理員，並決定是否將其列為資安事件調查。	II	◎	□ 適用 □ 不適用 說明：	
5. 加強網路安全管理					
5.1 網路通訊與資訊作業安全管理(II)					
5.1.1 任何對於客戶資料之查調、處理等作業，應於可滿足業務需求與合理人力分工之前提下，採用最小揭露與最小權限原則。					
5.1.1.1	對於安全要求高的資訊業務(如：牽涉客戶資料)，是否盡可能區隔其職務與責任領域？	II		□ 適用 □ 不適用 說明：	□ 備有職務分配表
5.1.1.2	營業用的電腦伺服器，是否盡可能授權不同的人員來執行用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作？	II		□ 適用 □ 不適用 說明：	
5.1.2 應對無線網路之使用進行規定並限制外來使用。					
5.1.2.1	無線網路基地台是否僅提供內部員工，以帳號密碼或金鑰傳輸等加密方式使用？	II		□ 適用 □ 不適用 說明：	
5.1.2.2	無線網路設備、基地台及管理伺服器，是否備有使用帳號申請紀錄，並定期執行密碼變更與設定足夠強度之加密金鑰？	II	◎	□ 適用 □ 不適用 說明：	
5.1.3 宜對公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，有相關的網站伺服器強化措施及定期執行網站技術弱點處理程序。					
5.1.3.1	若公司擁有或委外維運之對外公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，是否參考「電子商務交易安全規範-網路平台：5.3 交易網站伺服器強固」考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.1.3.2	若公司擁有或委外維運之對外公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，是否參考，「電子商務交易安全規範-網路平台：5.4 交易網站技術弱點管理」考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
5.2 電子郵件安全管理					
5.2.1 應對電子郵件程式進行相關安全設定，如需傳送客戶資料或訂單資料宜加密保護。					
5.2.1.1	敏感或機密性之客戶個資或交易資料，如需以電子郵件附件方式對外傳送，是否採用合宜的加密措施(如：壓縮軟體 RAR、ZIP 加上密碼等)處理後傳送？			□ 適用 □ 不適用 說明：	
5.2.1.2	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？			□ 適用 □ 不適用 說明：	
5.2.1.3	是否關閉電腦端郵件收發軟體(如：Outlook 或 Outlook Express)與 Webmail 的信件自動下載圖片(或其他內容)功能？			□ 適用 □ 不適用 說明：	
5.2.1.4	若使用電腦端郵件收發軟體(如：Outlook 或 Outlook Express)，是否採取純文字模式開啟郵件、關閉郵件預覽功能，或設定防毒軟體即時掃描以避免電子郵件夾帶病毒之風險？			□ 適用 □ 不適用 說明：	
5.2.2 應定期對執行電子商務作業之電子郵件帳號進行密碼變更要求。					
5.2.2.1	是否牢記並定期更改執行電子商務作業之電子郵件密碼以防止被盜用？			□ 適用 □ 不適用 說明：	
5.2.2.2	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？			□ 適用 □ 不適用 說明：	
5.2.3 應制定電子郵件使用規則，並對人員進行郵件使用宣導，以維護使用郵件的系統與應用程式的安全。					
5.2.3.1	使用者是否了解電子郵件社交工程威脅？	II		□ 適用 □ 不適用 說明：	□ 防範社交工程詐騙宣導說明

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.2.3.2	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？	II		□ 適用 □ 不適用 說明：	
5.2.4 應設置防止垃圾郵件或設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件。					
5.2.4.1	是否設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件？	II		□ 適用 □ 不適用 說明：	□ 設定郵件過濾規則
5.2.4.2	是否設定垃圾郵件過濾機制？	II	◎	□ 適用 □ 不適用 說明：	
5.2.4.3	是否考量禁止使用公司外部之電子郵件信箱或 Webmail 收發郵件？	II	◎	□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
5.2.4.4	電子郵件系統如需發送郵件到公司以外之網域，是否考量於郵件本文後加註隱私權、法律責任聲明等，以保障公司權益？	II	◎	□ 適用 □ 不適用 說明：	
6. 建立外部單位資料交換安全管理					
6.1 配送資料電子交換協議與保護					
6.1.1 應與電子商務網路平台(含平台商、物流商)及涉入電子商務交易流程之商業合作夥伴，協定各作業流程之電子資料交換機制(含資料往返、互換及二次以上傳遞)，並予以保護。(II)					
6.1.1.1	公司的資訊設備(如：主機、個人電腦等)與電子商務網路平台之系統連線通道(例如 FTP, SSL, 網站後台或其他遠端登入方式)，是否予以加密？	II		□ 適用 □ 不適用 說明：	□ 加密方式為：_____
6.1.1.2	是否透過帳號、密碼等識別方式以識別資料交換操作的使用者身份，且若有多名操作人員，是否以個別之帳號、密碼登入？	II		□ 適用 □ 不適用 說明：	□ 備有帳號申請紀錄 □ 未有帳號共用情
6.1.1.3	是否每季檢視交易資料交換操作人員之權限設定，以確認相關開放權限皆為職務所需？	II		□ 適用 □ 不適用 說明：	□ 備有每季權限審查紀錄
6.1.1.4	是否可依使用者需求，考量提供單次、每日或每月之資料交換報表查詢功能，確保傳輸資料之完整與正確性？	II		□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
6.1.1.5	與網路平台、物流商或金融單位的電子商務交易資料的交換軌跡是否已記錄，並妥善保存至少一年以上？	II	◎	□ 適用 □ 不適用 說明：	□ 備有資料交換紀錄 □ 保留期限少於一年
6.1.1.6	員工是否瞭解電子商務網路平台發放加密憑證之用途，並書面規定憑證安全與管理程序？	II	◎	□ 適用 □ 不適用 說明：	□ 備有書面規定 □ 未違反書面規定
6.1.2 宜限制高風險業務或敏感性資訊避免使用即時通訊軟體或外部電子郵件信箱進行資料傳輸作業。					
6.1.2.1	是否考量限制即時通訊相關軟體(如 MSN, Yahoo 即時通, Google talk)之使用？或監控其記錄與限制傳檔功能？	II	◎	□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
6.1.2.2	是否考量限制公司外部之電子郵件信箱或 Webmail 之使用？或監控其記錄與限制傳檔功能？	II	◎	□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
6.2 實體傳遞過程的保護					
6.2.1 應保護內有客戶資料之儲存媒體(如磁片、光碟片及磁帶)，連同消費者之貨品交寄皆應採用可靠之遞送管道並取得收訖證明。					
6.2.1.1	因業務需求，需利用郵遞交換內存客戶資料之儲存媒體時，是否先將媒體中之客戶資料予以加密？	II		□ 適用 □ 不適用 說明：	□ 加密方式為：_____
6.2.1.2	因業務需求，需利用郵遞交換內存客戶資料之儲存媒體時，是否將其裝入信封並密封後再行交付？			□ 適用 □ 不適用 說明：	
6.2.1.3	訂單資料或媒體交換是否專人遞送，或雇請優良商譽之快遞公司、郵局掛號交寄，並留存收訖證明？			□ 適用 □ 不適用 說明：	□ 有固定委託或契約快遞公司 □ 備有一個月內之收訖證明 □ 指定專人親送並留存簽收紀錄
7. 建立資安事件通報管理機制					
7.1 電子商務資安事件通報機制					
7.1.1 應建立「電子商務資安事件通報機制規範」通報方式之認知。					
7.1.1.1	是否確實了解「電子商務資安事件通報機制」所提供之服務與配合方式，並定期通報服務資訊予內部作業人員？			□ 適用 □ 不適用 說明：	
7.1.2 應參照「電子商務資安事件通報機制規範」，進行資安事故外部通報。(II)					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
7.1.2.1	是否確實了解「電子商務資安通報機制」所提供之服務與配合方式，並定期通報服務資訊予內部作業人員？	II		□ 適用 □ 不適用 說明：	
7.1.2.2	是否參考「電子商務資安通報機制規範」，建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常等)之外部通報與提報程序？	II	◎	□ 適用 □ 不適用 說明：	
7.1.2.3	是否具體落實外部通報作業？	II		□ 適用 □ 不適用 說明：	
7.1.2.4	是否隨時接收外部重大資安資訊，並立即採取必要反應行動？	II		□ 適用 □ 不適用 說明：	
7.2 資安事故管理					
7.2.1 應建立內部資安事件通報程序，並對內外部員工宣導相關通報流程。					
7.2.1.1	是否建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常等)與個資外洩危機通報與處理機制？	II	◎	□ 適用 □ 不適用 說明：	
7.2.1.2	員工及外部使用者是否知悉資安及個資外洩事件通報窗口及處理程序？	II		□ 適用 □ 不適用 說明：	□ 公告資安事件通報程序 □ 辦理人員認知訓練
7.2.2 應收集、保存及呈現資安事故之完整證據，並針對事故之原因進行檢討分析。					
7.2.2.1	是否建立資安事故管理機制，如記錄事故型式、處置方法、處理成本及矯正預防措施？	II		□ 適用 □ 不適用 說明：	
7.2.2.2	是否已建立及使用各項指標，以協助偵測安全事件，並預防安全事故？	II	◎	□ 適用 □ 不適用 說明：	
7.2.2.3	資安事件中相關證據資料是否有適當保護措施以作為問題分析及法律必要依據？	II		□ 適用 □ 不適用 說明：	
7.2.2.4	資安事件之回應小組是否被授權在處理事件時採取立即之決定？	II	◎	□ 適用 □ 不適用 說明：	□ 備有授權文件

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
7.2.2.5	資安事件之回應小組是否與外部團體(例如：執法機關、政府緊急應變中心、客戶、產業供應鏈上下游業者、電子商務資安事件通報機制等)建立一定之聯繫管道？	II	◎	□ 適用 □ 不適用 說明：	□ 備有外部聯絡清單
7.2.2.6	資訊安全事件處理的過程是否均留有完整紀錄？如有必要，應經由直接發送的電子郵件或網站首頁即時回報事件予相關產業供應鏈上下游業者與消費者。	II	◎	□ 適用 □ 不適用 說明：	□ 備有資安事件紀錄

資料來源：本計畫整理

陸、附錄

一、參考文件索引表

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
策略目標：1. 促進組織資訊安全管理			
1.1 資訊安全框架	1.1.1	ISO 27001 A.6.1.1	
		ISO 27001 A.6.1.3	
1.2 資訊資產風險管理	1.2.1	ISO 27001 4.2	「電子商務交易安全規範-網路平台」
		ISO 27001 A.7	「電子商務交易安全規範-網路平台」
		ISO 27001 A.14	「電子商務交易安全規範-網路平台」
1.3 人力安全管理	1.3.1.	ISO 27001 A.8.1.3	
		ISO 27001 A.8.2.2	
		ISO 27001 A.8.3.2	
		ISO 27001 A.8.3.3	
1.4 遵循性管理	1.4.1	ISO 27001 A.15	
1.5 客戶及第三方管理	1.5.1	ISO 27001 A.6.2	
		ISO 27001 A.6.2.1	
		ISO 27001 A.6.2.2	
		ISO 27001 A.8.1.3	
		ISO 27001 A.6.2.3	
		ISO 27001 A.10.2.1	
		ISO 27001 A.10.2.3	
策略目標：2. 加強營業資訊設備管理			
2.1 營業資訊設備使用及安全管理	2.1.1	ISO 27001 A.10.4.1	
		ISO 27001 A.10.4.2	
	2.1.2	ISO 27001 A.10.5.1	
	2.1.3	ISO 27001 A.10.10.6	
2.2 使用電子商務網路交易平台之存取授權管理	2.2.1	ISO 27001 A.11.2.1 ISO 27001 A.11.2.3	
	2.2.1	ISO 27001 A.8.3.3	
		ISO 27001 A.11.3.	
		ISO 27001 A.11.5.2	
	2.2.2	ISO 27001 A.6.2	「電子商務交易安全規範-網路平台」
策略目標：3. 保護客戶個資及營業資料安全			
3.1 客戶個人資料保護	3.1.1	ISO 27001 A.15.1.4	
		ISO 27001 A.15.1.4	「零售業等網路交易定型化契約應記載及不得記載事項」
	3.1.2		個人資料保護法
3.2 客戶個資及營業資料之作業	3.2.1	ISO 27001 A.10.7.3	
		ISO 27001 A.10.5.1	

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
安全		ISO 27001 A.11.3.3	
		ISO 27001 A.11.3.2	
		ISO 27001 A.15.2.1	
			「電子商務交易安全規範-網路平台」
	3.2.2	ISO 27001 A.10.7.3	
3.3 公開交易資訊管理	3.3.3	ISO 27001 A.10.9.1 A.10.9.3	「零售業等網路交易定型化契約應記載及不得記載事項」
		ISO 27001 A.10.9.2	
3.4 配送作業之紙本資料管理	3.4.1	ISO 27001 A.6.2	
		ISO 27001 A.15.1.4	
		ISO 27001 A.11.3.3	
		ISO 27001 A.10.7.3	
	3.4.2	ISO 27001 A.10.7.3	
		ISO 27001 A.10.10.1	
		ISO 27001 A.11.4.6	
策略目標：4. 加強作業環境安全管理			
4.1 作業與辦公環境安全管理	4.1.1	ISO 27001 A.9.1.1	
		ISO 27001 A.9.1.2	
		ISO 27001 A.9.1.3	
		ISO 27001 A.9.1.4	
	4.1.2	ISO 27001 A.8.3.2	
		ISO 27001 A.9.1.2	
		ISO 27001 A.10.10.1	
		ISO 27001 A.13.1.1	
		ISO 27001 A.9.2.1	
		ISO 27001 A.9.2.5	
4.2 電腦設備環境與設備安全管理	4.2.1	ISO 27001 A.9.2.6	
	4.2.2	ISO 27001 A.9.1.2	
		ISO 27001 A.9.2.1	
		ISO 27001 A.9.2.3	
		ISO 27001 A.9.2.2	
		ISO 27001 A.9.2.4	
			「電子商務交易安全規範-網路平台」
	4.2.3	ISO 27001 A.10.1.2	
		ISO 27001 A.10.7.1	
		ISO 27001 A.10.7.3	
		ISO 27001 A.11.3.3	
		ISO 27001 A.15.1.5	
		ISO 27001 A.13.1.1	
4.3 使用者應遵守安全要求之管理	4.3.1	ISO 27001 A.12.4.1	
		ISO 27001 A.11.3.1	
		ISO 27001 A.11.3.3	
		ISO 27001 A.11.4.6	

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
		ISO 27001 A.10.10.2	
策略目標：5. 加強網路安全管理			
5.1 網路通訊與資訊作業安全管理	5.1.1	ISO 27001 A.10.1.3	
	5.1.2	ISO 27001 A.11.4.1	
	5.1.3		「電子商務交易安全規範-網路平台」
5.2 電子郵件安全管理	5.2.1	ISO 27001 A.10.8.4	
		ISO 27001 A.10.6.1	
	5.2.2	ISO 27001 A.11.3.1	
	5.2.3	ISO 27001 A.8.2.2	
		ISO 27001 A.10.4.1	
	5.2.4	ISO 27001 A.10.6.1	
		ISO 27001 A.11.4.6	
		ISO 27001 A.15.1.3	
策略目標：6. 建立外部單位資料交換安全管理			
6.1 配送資料電子交換協議與保護	6.1.1	ISO 27001 A.10.8.1	
		ISO 27001 A.12.3.1	
	6.1.2	ISO 27001 A.11.4.6	
6.2 實體傳遞過程的保護	6.2.1	ISO 27001 A.10.8.3	
策略目標：7. 建立資安事件通報管理機制			
7.1 電子商務資安事件通報機制	7.1.1	ISO 27001 A.13.1	「電子商務資安通報機制規範與作業要點」
	7.1.2	ISO 27001 A.13.1	「電子商務資安通報機制規範與作業要點」
7.2 資安事故管理(II)	7.2.1	ISO 27001 A.13.1	
	7.2.2	ISO 27001 A.13.2	

二、規範常見名詞釋義

項次	名詞	定義說明	備註
1	風險評鑑	風險分析與風險評估的整個過程。	
2	風險	威脅利用弱點對資訊資產所造成影響之可能性。	
3	風險評估	把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。	
4	風險分析	系統性的使用資訊，以識別緣由與估計風險。	
5	威脅	危及資訊資產的外在因素，如天然災害、惡意攻擊等。	
6	脆弱點	指資訊資產內部可能遭受威脅利用之處。	
7	螢幕淨空	當設備無人看管或使用時宜將個人電腦和終端機	

項次	名詞	定義說明	備註
		保持在登出或鎖定狀態，以通行碼等授權機制保護的螢幕及鍵盤上鎖機制保護。	
8	惡意程式、惡意碼	故意建立用來執行未經授權並通常是有害行為的軟體程序，包括病毒、後門程序、鍵盤紀錄器、密碼盜取者和其它木馬程序、Word 和 Excel 病毒、木馬、犯罪軟體、間諜軟體和廣告軟體。	
9	行動碼	由遠端系統透過網路轉存入本機端進行代理作業，可進行下載或在本機端上執行沒有明確安裝或者接受者的作業。包括 include scripts(Java 腳本，VBScript)、Java 小應用程式，ActiveX 控制，flash 動畫。	
10	安全容量	系統或網路的資源使用宜監控、調校、及預估未來容量需求，以確保服務可有效運作。	
11	時間同步	業務營運相關系統宜與議定的準確時間(如中原標準時間、NTP 或其他公正單位)進行時間校正與同步作業。	
12	委外廠商	第三方委外單位、第三方合作業者，含物流商、供應商及服務商等。	
13	利害相關團體	執法機關、政府緊急應變中心、客戶、產業供應鏈上下游業者、電子商務資安事件通報機制	
14	儲存媒體	資料儲存媒介，例如：紙本文件、電腦媒體(磁片、磁帶、記憶卡、外接硬碟與光碟片)。	
15	可攜式設備	包括筆記型電腦、PDA 等	
16	密碼、加密	Cryptographic，將正常的(可識別的)資訊轉變為無法識別的信息。	
17	通行碼	Password，對應帳號的登入密碼，使用者在存取資訊系統與服務前，依使用者授權用來查證其身份的方法。	
18	資訊安全事件	information security event 系統、服務或網路狀態經鑑別而顯示示可能有違反資訊安全政策或保護措施失效，或可能與安全有關但事先未知狀況的發生	
19	TWCA	臺灣網路認證公司，提供國內網路安全認證服務，為國內最大的民間憑證發行機構。	
20	PCIDSS	Payment Card Industry Data Security Standard，支付卡產業相關標準指引與要點，由 Visa International、MasterCard Worldwide、 American Express、Discover Financial Services 及 JCB 等支付卡產業安全標準委員會提出，目的在幫助公司保護支付卡帳戶資料。	1.2.1 版，2009 年 7 月版
21	保密協議	透過保密切結書、合約書等文件規範相關保密要	參照 ISO

項次	名詞	定義說明	備註
		求。	27002-6.1.5
22	社交工程	利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。	
23	即時通訊軟體	如 msn、yahoo 即時通、Google Talk、Skype 等軟體，可使用網路即時的傳遞文字訊息、檔案、語音與視訊交流。	

物流商交易安全規範

經濟部商業司

電子商務交易安全規範
物流商
規範、進階指引及查檢表

V3.0 版

指導單位：經濟部商業司
主辦單位：財團法人資訊工業策進會
執行單位：中華無店面商務發展協會
中 華 民 國 １０１ 年 １０ 月

目　錄

圖目錄

表目錄

壹、前言

一、依據

經濟部商業司(下稱商業司)「101 年度電子商務交易安全及資安服務平台推動計畫」(下稱本計畫)。

二、主旨

為提升電子商務供應鏈之電子商務平台業者之資訊安全管理、商品供應商(或賣家)的資訊管理與物流商資訊管理流程等之作業安全需求，特召集產業代表、專家學者、顧問單位共同參與規劃、審查並修正「電子商務交易安全規範」(下稱本規範)，做為我國電子商務產業相關業者之行政參考文件，本規範依實施對象分別編纂 3 份規範文件：

(一) 電子商務交易安全規範-網路平台 1 式

(二) 電子商務交易安全規範-供應商 1 式

(三) 電子商務交易安全規範-物流商 1 式

以有助於電子商務業者致力提升交易安全、強化消費者安全信賴時，於各項管理面、作業面之實務參考。

三、電子商務定義

我國行政院主計總處所編印之「中華民國行業標準分類」，其主要目的在於提供統計分類之用，行業標準分類原則主要係參酌聯合國國際行業標準分類(International Standard Industrial Classification of All Economic Activities, ISIC)中以場所單位之主要經濟活動作為分類基礎之架構。其中關於電子商務之定義，依據聯合國國際行業標準分類第 4 次修訂版(ISIC Rev.4)之定義為:「企業單位接到訂單後，

以各種電子媒介方式處理所生產之商品及服務之交易，例如藉由電話、傳真、電視、電子資料交換(EDI)及網際網路。」亦即所有從事商品或服務之所有權移轉，是藉由網際網路或其他的電子媒介所為的商業交易行為就稱之為電子商務。

另依據商業司在「2011 電子商務年鑑」，將電子商務定義為：「運用先進資訊科技，同時藉由組織作業的流程改造，來達到減低組織營運的成本開支，提升作業效率，增加客戶滿意度之商業活動。」亦即利用電腦或新興手持式電子產品，例如智慧型手機、平版電腦等，透過網路進行買賣交易之行為皆稱之為「電子商務」。如商業EDI(Electronic Data Interchange)、金融 EDI、網路銀行、網路購物等行為，都涵蓋在電子商務範疇之中。

四、目的

本規範文件之制定，除參考我國資通安全管理相關規範、CNS 27001:2005 資訊安全管理標準、個人資料保護法及其他國際標準中與電子商務產業相關的規範，據以規劃本規範文件之框架，並依據以下目的，訂定適合企業交易安全實務操作之文件。

(一) 依電子商務業者之營業額、個資量、作業特性等分級分類，不同等級給予不同的資安防護實施建議。

(二) 3 份交易安全規範，至少涵蓋以下作業流程，以利電子商務業者掌握上下游作業之資訊安全。

1. 電子商務供應鏈之中大型電子商務平台業者之資訊安全管理。
2. 含內部資訊流管理。
3. 交易網站安全機制管理。

4. 有效的交易網站安全機制。

5. 與供應鏈的協同資訊作業管理。

6. 商品供應商(或賣家)的資訊管理(含交易資訊管理流程)。

7. 物流商資訊管理流程(含客戶資料保護管理)。

8. 作業安全需包含交易資訊之機密性、交易平台之可用性、交易內容之完整性、與交易作業之適法性等需求。

貳、文件說明

一、適用範圍

(一)「電子商務交易安全規範-網路平台」適用對象為電子商務平台業者，其類型包含如下，並不加以第一類、第二類區分，規範要求皆適用。

1.B2C 平台商：使用電子商務技術，直接提供消費者商品購買服務之廠商。

2. B2B2C 平台商：提供網路交易平台，由個別網路商家參與，使用電子商務技術，直接或間接提供消費者購買服務之廠商。

(二)「電子商務交易安全規範-供應商」適用對象為配合網路平台電子商務交易，提供直接或間接 B2C 商品經銷或銷售之代理業者、經銷業者、零售業者或電子商家。不涉入 B2C 商品交易之訂購服務、客服服務、金流作業、配送服務等流程之商品製造、輸入、代理、經銷或銷售等業者，不包含在本規範之適用範圍中。

1. 第一類供應商：只有擁有一般網際網路連線、使用一般網站(Web)交易系統及一般辦公室使用之 OA 電腦設備之供應商。

2. 第二類供應商：擁有或租賃或委外之網際網路專線、營運系統或其他與電子商務相關應用系統之供應商，或與網路平台、物流商之間，透過後台連線交換傳遞或拋轉客戶之會員資料、訂購資料、交易金額、配送資料之供應商。

(三)「電子商務交易安全規範-物流商」適用對象為配合網路平台電子商務交易，提供直送或轉運 B2C 境內(含離島)商品配送服務流程之汽機車快遞業者、路線貨運業者、宅配業者、郵遞業者，

以及提供取貨服務之實體商店等。跨境之海陸空運承攬業者、倉儲流通轉運業者、大型批發物流流通業者等不涉入 B2C 商品配送服務的作業流程，不包含在本規範適用範圍。

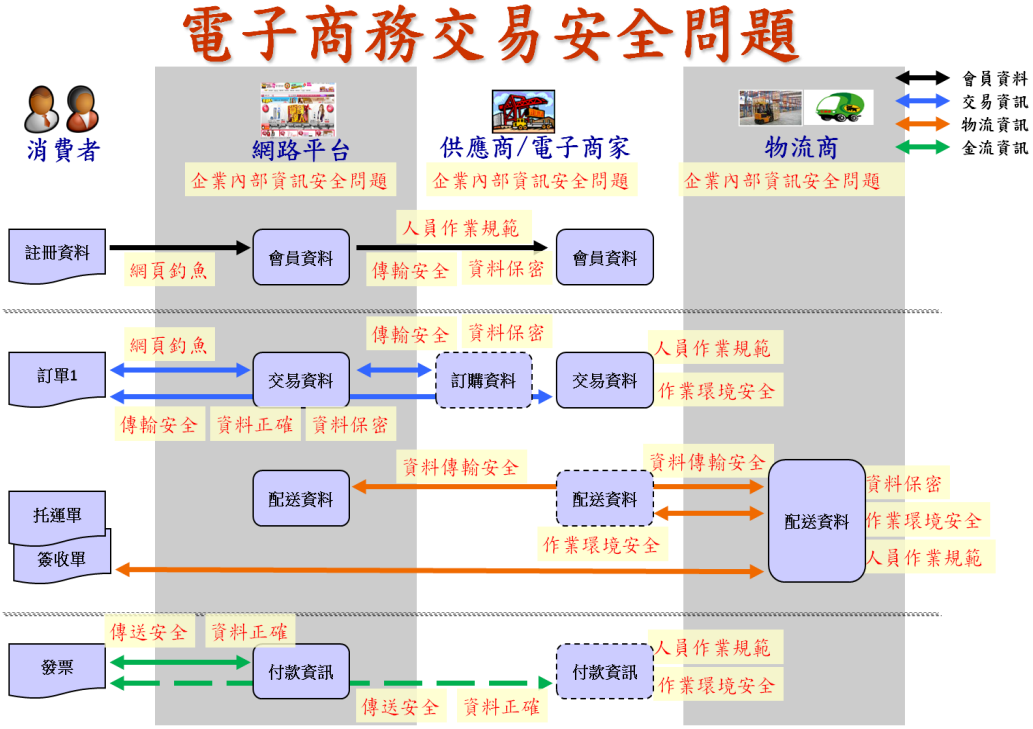
1. 第一類物流商：僅接觸紙本(含印出之配送單、簽收單及手寫快遞單正副本)配送資料之物流商。
2. 第二類物流商：與網路平台、供應商之間，有連線或離線的電子資料交換、傳送等作業流程之物流商，或其本身擁有物流服務網路平台、物流配送作業管理系統等之物流商。

二、規範之文件位階

本規範主要為電子商務產業專用之二階規範暨三階指引。二階規範定義為電子商務業者依據分級所必要遵循或執行之安全作為；規範內容多數係依據相關法令法規與國際標準要求制定。三階指引將提供電子商務業者為強化交易安全與客戶資料保護之進階資安作為參考；規範內容係依據國內外各項資安實作手冊制定，並參考連結至商業司相關資安規範。

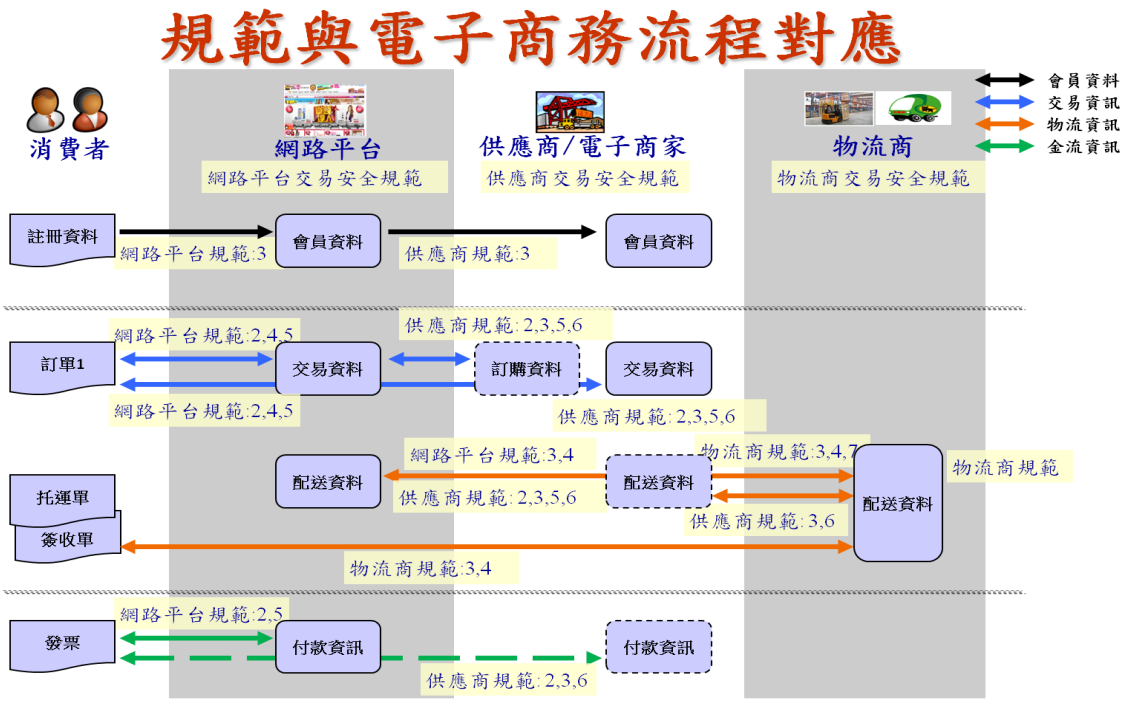
三、規範之實施策略目標

依據規範適用範圍之電子商務業者，所涵蓋之交易服務上下游作業流程，為確保實施 3 份規範能達成之交易安全提升，爰依據上下游作業流程中，應予以保護之重要資訊流(如圖 1、2，表 1)，訂定相對應之實施策略目標。



資料來源：本計畫整理

圖 1　交易服務上下游作業流程重要資訊流與安全問題



資料來源：本計畫整理

圖 2　交易服務上下游作業流程與規範實施策略目標對照

表 1　電子商務交易安全規範實施策略目標

文件名稱	電子商務交易安全規範-網路平台	電子商務交易安全規範-物流商	電子商務交易安全規範-供應商
實施策略目標	1 促進組織資訊安全管理	1.促進組織資訊安全管理	1.促進組織資訊安全管理
	2.加強核心營運系統與資料庫之安全管理	2.加強核心資訊系統安全管理	2.建立營業資訊設備管理
	3.強化客戶個人資料安全管理	3.保護客戶個人資料檔案安全	3.保護客戶個資及作業資料安全
	4.提升企業內資訊環境安全管理	4.建立託運單安全管理	
		5.加強作業環境安全管理	4.加強作業環境安全管理
		6.加強網路安全管理	5.加強網路安全管理
	5.強化對外網站交易平台安全管理	7.建立外部單位資料交換安全管理	6.建立外部單位資料交換安全管理
	6.建立資安通報管理機制	8.建立資安通報管理機制	7.建立資安通報管理機制

資料來源：本計畫整理

四、資訊安全框架

因 ISO 27001/ISO 27002 之資安管理領域架構，為國內與國際最多機構(含電子商務產業)之產業資安標準之參考框架，因此將之列為本規範框架之主要依據。

為補足 ISO 27002 之實作指引對個資管理的深度不足，本規範將另行依據最新之個資法所規範之管理精神，強化電子商務產業客戶個資管理。

五、規範文件結構

(一) 文件結構

為依循電子商務產業特性，以制定管理面、作業面的可達成之原則性的交易安全規範。故將規範文件分為策略目標、規範大綱、要求項目與進階指引共四層之文件結構。

(二) 規範共分為四層：

1. 第一層為提升電子商務交易安全之策略目標；
2. 第二層為達成個策略目標之管理項目；
3. 第三層為各管理項目下之具體要求項目；
4. 第四層為達成要求項目之必要或參考查檢表；查檢表之檢核紀錄欄位亦列出於交易安全執行現況中，可作為佐證資訊之相關建議，以提供業者實施本規範之操作面參考。

表 2　規範內容示例

管理項目	要求項目	類別	依據之法規或標準
策略目標：1.促進組織資訊安全管理			
1.3 資訊安全框架	1.1.5 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。	皆適用	ISO 27001
	1.1.6 電子商務網路平台管理階層，應具體說明其對資安之承諾與責任。	皆適用	ISO 27001

資料來源：本計畫整理

(三) 查檢表

1. 為有利於網路平台業者依營運現況進行分類分級實施，並使企業自我檢查或外部第三方查核能有所依據，爰依照各要求項目制定查檢表。除前述之基本遵守的規範要求以外，特於查檢表中訂定進階指引操作項目，以提供企業參考使用。
2. 查檢表中標示“II”表示僅第二類業者適用。

3. 針對各項規範要求，本規範提供業者必要執行之作業基準查檢項目，及進階查檢項目(進階指引欄位標示◎)。

4. 作業基準查檢項目(Baseline，簡稱 BL)，係為達成各要求項目之交易安全風險基礎管理工作，業者必要且至少應執行之控管作為。

5. 進階查檢項目(Better Practice，簡稱 BP)，係依據各項國際資安實務準則，提供業者參考之進階控管作為，業者得依據資源與風險現況自行決定是否執行。

表 3　查檢表內容示例

編號	要求之查檢項目	類別	進階指引	檢核結果	檢核紀錄
1. 促進組織資訊安全管理					
1.1 資訊安全框架					
1.1.1 電子商務網路平台應擬定資安政策，並依據政策落實資安管理、定期稽核與進行有效性量測並公告周知(含員工、委外廠商、上下游合作廠商)。					
1.1.1.1	是否制定全公司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)？			□ 符合 □ 不符合	□ 制定政策，內容包含： - 資訊安全的目標 - 概要資訊安全原則的需求 - 公司內部權責 □ 政策公告內部員工 □ 政策公告給外部廠商 □ 政策定期審查與更新

資料來源：本計畫整理

(四) 附錄

為利於業者對照 ISO 27001、ISO 27002、個人資料保護法以及

規範中參考引用之其他管理標準，將規範依查檢項目編號與其對應之法規或標準以及其他可供規範時做參考來源，編列參考文件索引表於附錄中。

另將 3 份規範常見名詞，增列其名詞釋義表於附錄中，但未以所有相關標準出現名詞為涵蓋範圍。

六、未盡事宜

本規範制定時依產業現況與需求，考量文件位階、制定目標、適用範圍及業者實施可能遭遇困難及資源限制，以及目前相關法令法規、產業標準版本發布內容等因素，其有未盡事宜，非為規範之執行限制。已導入相關資訊安全標準之業者，仍建議以符合企業經營及競爭力提升之需求，充分涵括電子商務交易安全相關作業流程或企業整體資訊安全管理流程，施予應有及必要之安全保護，以利電子商務信賴安全環境之發展。

參、規範概述

一、整體大綱

本(物流商)交易安全規範 8 大實施策略目標下，共計 25 個管理項目，55 條要求規範，皆為應執行之作業基準(Baselines)。規範之下共提供 264 條查檢項目供業者查檢之參考，其中 116 條為第一類業者適用(僅需)查核之項目，其餘 148 條為第二類業者適用查核項目。第二類業者適用查核項目中，亦有 81 條進階指引(Better Practices)之查檢項目，可依據風險管理需求選擇性執行，或依實際執行情形記錄查檢結果。

二、規範導入及 ISO 27001 符合性說明

本(物流商)交易安全規範 8 大實施策略目標與 ISO 27001 管理領域之對照如下，通過 ISO 27001 驗證之業者，可依其資訊安全管理制度適用性聲明文件中，已適用之管理領域與控制項目，對照規範管理項目，以有助於確認規範符合性或強化既有資訊安全管理制度之參考。

表 4　物流商交易安全規範實施範圍

策略目標	管理項目	實施範圍	規範項目數
1.促進組織資訊安全管理	1.1 資訊安全框架 1.2 資訊資產風險管理 1.3 人力安全管理 1.4 遵循性管理 1.5 客戶及第三方管理	- 管理階層 - 人力資源管理部門(包含委外廠商) - 法律遵循性管理部門(包含智慧財產權、個人資料保護法、消費者保護法等) - 資產風險管理部門	8
2.加強核心資訊系統安全管理	2.1 核心資訊系統取得、開發及維護安全管理	- 負責物流作業管理系統或重要核心營運系統維運之管理	10

策略目標	管理項目	實施範圍	規範項目數
	2.2 核心資訊系統存取控制管理 2.3 核心資訊系統資料庫安全管理	部門 - 負責系統開發、系統存取控制、機房與作業環境、營運持續等作業流程之執行單位	
3.保護客戶個人資料檔案安全	3.1 客戶資料隱私管理原則 3.2 客戶資料依法對外公開、資訊揭露作業 3.3 客戶資料取得、處理、儲存及其機密性與正確性管理 3.4 客戶資料使用及傳輸安全作業 3.5 客戶資料刪除及停止利用作業	- 涉及消費者個人資料之作業部門與其作業流程	12
4.建立託運單安全管理	4.1 託運單資料管理 4.2 紙本託運單之保存及銷毀管理 4.3 託運單調閱與印製作業管理	- 涉及電子商務 B2C 交易商品配送服務，或接觸、存取、使用、保存、管理託運單之作業部門與其作業流程	4
5.加強作業環境安全管理	5.1 作業與辦公環境安全管理 5.2 營業用電腦設備環境與設備安全管理	- 負責公司辦公作業環境管理、資訊作業環境管理之執行單位 - 負責營業用電腦設備管理之執行單位	4
6.加強網路安全管理	6.1 網路通訊與資訊作業安全管理 6.2 電子郵件安全管理	- 負責公司整體網路通訊、資訊作業環境管理之執行單位 - 所有使用企業與電子商務配送服務相	12

策略目標	管理項目	實施範圍	規範項目數
	6.3 個人資訊設備安全管理	關業務之使用者	
7.建立外部單位資料交換安全管理	7.1 配送資料交換協議與保護措施 7.2 配送資料傳遞過程的儲存媒體保護	- 涉及與外部單位進行資料交換之作業單位 - 提供或支援與外部單位資料交換設備之作業單位	2
8.建立資安通報管理機制	8.1 電子商務資安通報機制 8.2 資安事故管理	- 管理階層 - 負責資訊安全事故管理執行單位	3
		小計	55

資料來源：本計畫整理

表 5　物流商交易安全規範與 ISO 27001 符合性對照

策略目標	管理項目	ISO 27001 管理領域對照
1.促進組織資訊安全管理	1.1 資訊安全框架 1.2 資訊資產風險管理 1.3 人力安全管理 1.4 遵循性管理 1.5 客戶及第三方管理	- 本文(4.2, 4.3,6) - 組織管理(A.6) - 資產管理(A.7) - 人員安全管理(A.8) - 通訊與作業管理(A.10) - 遵循性管理(A.15)
2.加強核心資訊系統安全管理	2.1 核心資訊系統取得、開發及維護安全管理 2.2 核心資訊系統存取控制管理 2.3 核心資訊系統資料庫安全管理	- 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12)

策略目標	管理項目	ISO 27001 管理領域對照
3.保護客戶個人資料檔案安全	3.1 客戶資料隱私管理原則 3.2 客戶資料依法對外公開、資訊揭露作業 3.3 客戶資料取得、處理、儲存及其機密性與正確性管理 3.4 客戶資料使用及傳輸安全作業 3.5 客戶資料刪除及停止利用作業	- 人員安全管理(A.8) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 遵循性管理(A.15)
4.建立託運單安全管理	4.1 託運單資料管理 4.2 紙本託運單之保存及銷毀管理 4.3 託運單調閱與印製作業管理	- 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 存取控制管理(A.11) - 資訊系統開發及維護管理(A.12) - 遵循性管理(A.15)
5.加強作業環境安全管理	5.1 作業與辦公環境安全管理 5.2 營業用電腦設備環境與設備安全管理	- 人員安全管理(A.8) - 實體與環境安全管理(A.9) - 通信與作業管理(A.10) - 資訊安全事故管理(A.13) - 遵循性管理(A.15)
6.加強網路安全管理	6.1 網路通訊與資訊作業安全管理 6.2 電子郵件安全管理 6.3 個人資訊設備安全管理	- 通信與作業管理(A.10) - 存取控制管理(A.11) - 遵循性管理(A.15)
7.建立外部單位資料交換安全管理	7.1 配送資料交換協議與保護措施 7.2 配送資料傳遞過程的儲存媒體保護	- 通信與作業管理(A.10) - 資訊系統開發及維護管理(A.12)
8.建立資安通報管理機制	8.1 電子商務資安通報機制 8.2 資安事故管理	- 資訊安全事故管理(A.13)

資料來源：本計畫整理

肆、規範內容

說明：

本節為本規範要求項目所有內容，其表列順序依照第參章第一節整體大綱，內容涵括規範之第一層至第三層，並標示每一條規範之適用業者分類類別以及依據之法規或標準名稱。

表 6　物流商交易安全規範要求項目表

管理項目	要求項目	類別	依據之法規或標準
策略目標：1.促進組織資訊安全管理			
1.1 資訊安全框架	1.1.1 物流商應擬定資安政策，由管理階層具體說明其對資安之承諾與責任，並依據政策落實資安管理。	皆適用	ISO 27001
	1.1.2 物流商宜訂定資安與個人資料管理之稽核程序，設置稽核人員定期進行內部稽核作業，並於後續進行追蹤與改善。	皆適用	ISO 27001
1.2 資訊資產風險管理	1.2.1 物流商宜建立適當之資產管理機制，分析其作業流程之資安風險與建立因應對策；並針對核心營運流程中斷之機率及衝擊進行評估，落實必要之營運持續計畫。	皆適用	ISO 27001
1.3 人力安全管理	1.3.1 物流商宜針對相關作業人員之可能偏差行為(如資料盜取或操作錯誤)，預先具體約束與控管。	皆適用	ISO 27001
	1.3.2 物流商應針對相關作業人員進行資安與個人資料保護的教育訓練與宣導。	皆適用	ISO 27001
	1.3.3 物流商應針對相關作業人員之資訊存取權限進行控管。	皆適用	ISO 27001
1.4 遵循性管理	1.4.1 物流商之資安作為應遵守民法、刑法、消保法、智慧財產權與個資法等相關法令法規，並滿足所提供之服務契約要求。	皆適用	ISO 27001
1.5 客戶及第三方管理	1.5.1 於上、下游電子資料交換協同作業中(含資料往返、互換及二次以上傳遞)，應確保作業之資訊安全，並與委外廠商於簽訂合約時訂定保密條款。	皆適用	ISO 27001
策略目標：2.加強核心資訊系統安全管理			
2.1 核心資訊系統取得、開發及維護安全	2.1.1 物流商的新資訊系統或現有資訊系統中，為了保障安全宜考量以文件詳述資訊安全之要求。	皆適用	ISO 27001
	2.1.2 輸入核心資訊系統的資料應透過程式邏輯設計予以檢查，確保資料正確。	皆適用	ISO 27001

管理項目	要求項目	類別	依據之法規或標準
管理	2.1.3 核心資訊系統的作業系統之升級或更新應有適當的管制，更新前應進行測試，測試環境宜予以獨立，並避免以真實客戶資料進行。	皆適用	ISO 27001
	2.1.4 核心資訊系統應於新功能上線或變更時執行測試，測試內容應同時考慮系統功能、可用性及安全性。	皆適用	ISO 27001
2.2 核心資訊系統存取控制管理	2.2.1 核心資訊系統應有足夠強度的帳號密碼申請及管理規定，使用者、系統管理者帳號及權限皆應有申請核准紀錄，及離調職時取消帳號紀錄。	皆適用	ISO 27001
	2.2.2 重要作業職權(如處理個資相關作業)應加以區隔，以降低資產遭未經授權或非意圖的修改或誤用之機會。	皆適用	ISO 27001
	2.2.3 核心營運系統之公用程式應用(如遠端連線程式、外部連線存取等)應進行管制。	皆適用	ISO 27001
2.3 核心資訊系統資料庫安全管理	2.3.1 核心資訊系統的資料庫應建立連線管制與存取控制機制，以保護消費者資料與交易資訊。	皆適用	ISO 27001
	2.3.2 核心資訊系統的資料庫應定期查檢，以保護消費者資料與交易資訊之正確與完整。	皆適用	ISO 27001
	2.3.3 核心資訊系統之資料庫應定期備份，並留存重要存取紀錄。	皆適用	ISO 27001
策略目標：3. 保護客戶個人資料檔案安全			
3.1 客戶資料隱私管理原則	3.1.1 應於網站或公司營運據點所屬範圍之適當地點公告隱私權保護宣告或政策，相關資訊至少包含客戶資料蒐集與利用範圍、第三方協同作業範圍、資料保護安全措施等。	皆適用	ISO 27001
	3.1.2 宜依相關法令指定專人辦理安全維護及客戶個人資料保管事項，且設置對外公告「客戶個人資料保護聯絡窗口」，協調聯繫客戶資料事宜，及擔任消費者提出申訴與救濟時之單一窗口。	皆適用	「個人資料保護法」
	3.1.3 宜定期盤點物流業務所涉及的客戶個人資料之敏感等級、儲存使用方式、傳輸媒介、接觸人員等，並評估其可能遭遇的重大風險，建置相對應的安全維護措施強度。	皆適用	「個人資料保護法」
3.2 客戶資料依法對外公開、資訊揭露作業	3.2.1 應依據法律規定、契約及正式對外宣告之隱私權政策，並於蒐集時即告知客戶相關訊息，始得執行客戶個人資料對外公開、資訊揭露等作業。	皆適用	「個人資料保護法」
	3.2.2 宜訂定包含所有線上及離線作業之客戶個人資料保護相關程序，規定客戶資料對外公開、資訊揭露作業之期間、地區、對象、處理方式與保護範圍(界	皆適用	「個人資料保護法」

管理項目	要求項目	類別	依據之法規或標準
	定交易網頁由平台業者或委外第三方單位控管)。		
3.3 客戶資料取得、處理、儲存及其機密性與正確性管理	3.3.1 取得、處理或利用客戶個人資料時，應依照法令規定及契約要求，透過文字描述其合理關連之特定目的、使用方式及消費者個人資料相關權利之行使方式，並取得當事人同意；變更使用目的或方式時亦需重新取得同意。	皆適用	「個人資料保護法」
	3.3.2 客戶個人資料之處理行為應經權責單位核准，並對處理客戶資料人員存取權限進行控管。	皆適用	ISO 27001
	3.3.3 應對客戶提出其個人資料查詢、更新與申訴等服務時，有完整的執行步驟與客戶回應說明。如客戶欲維護個人資料之正確性或發生爭議時，尊重消費者權益與意願，立即停止處理或利用，並於 30 日內予以回應處理狀況。	皆適用	「個人資料保護法」
	3.3.4 利用電腦處理客戶個人資料時，應有內部作業查驗程序，以確保輸入資料與原資料相符合。	皆適用	ISO 27001
3.4 客戶資料使用及傳輸安全作業	3.4.1 物流客戶個人資料之使用、傳遞與交換作業，應有加密或其他適當保全機制，並明確規定執行作業之期間、地區、對象、申請及處理方式。	皆適用	ISO 27001
3.5 客戶資料刪除及停止利用作業	3.5.1 含有客戶資料之儲存媒體，淘汰報廢時，應使用格式化或其他實體破壞方式予以銷毀。	皆適用	ISO 27001
	3.5.2 應控管配送作業相關客戶個人資料留存的時間，定期由專人或負責人員刪除，並由主管不定期抽檢。	皆適用	ISO 27001
策略目標：4.加強託運單安全管理			
4.1 託運單資料管理	4.1.1 客戶託運單應避免出現完整之客戶資訊，並對電子託運資料進行保護與備份。	皆適用	ISO 27001
4.2 紙本託運單之保存及銷毀管理	4.2.1 紙本託運單應集中保存，並僅限授權人員使用或進出集中保管處。	皆適用	ISO 27001
	4.2.2 準備丟棄作廢或不再持有之託運單或客戶配送單與簽收單等紙本資料，應使用碎紙機或其他實體破壞方式予以確實銷毀，或委由專業處理廠商於專人監督下銷毀。	皆適用	ISO 27001
4.3 託運單調閱與印製作業管理	4.3.1 託運單調閱應經過申請與授權，並限制託運單列印電腦環境。	皆適用	ISO 27001
策略目標：5.加強作業環境安全管理			

管理項目	要求項目	類別	依據之法規或標準
5.1 作業與辦公環境安全管理	5.1.1 應確保作業與辦公場所、託運單儲存及電腦設備機房區域之安全，避免竊盜或損害。	皆適用	ISO 27001
	5.1.2 除機房與辦公區域外，如倉儲站所等配送資料處理地點之設備應設計安全措施，保護場所管控外設備之安全。	皆適用	ISO 27001
5.2 營業用電腦設備環境與設備安全管理	5.2.1 應設計安全措施，確保營業用電腦伺服器與網路設備之安全，避免竊盜或損害。	皆適用	ISO 27001
	5.2.2 設備外送或淘汰前應進行安全措施，防止資訊外洩。	皆適用	ISO 27001
策略目標：6.加強網路安全管理			
6.1 網路通訊與資訊作業安全管理	6.1.1 營業用電腦設備應安裝防毒軟體，並定期更新病毒碼及執行系統掃描作業。	皆適用	ISO 27001
	6.1.2 應定期進行營業用資訊系統與軟體的備份與還原測試。	皆適用	ISO 27001
	6.1.3 應定期檢測網路安全及對外客戶託運資訊查詢網站之頻寬，以確保網路系統安全與連線品質。	皆適用	ISO 27001
	6.1.4 營業用電腦伺服器應安裝防火牆或入侵偵測系統，定期檢查防火牆和路由器的規則設定，以保護系統之安全。	皆適用	ISO 27001
	6.1.5 宜記錄使用者活動、異常及資訊安全事件，保留一段議定期間，以協助未來的調查與存取控制監視。	皆適用	ISO 27001
	6.1.6 所有交易相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。	皆適用	ISO 27001
	6.1.7 宜對公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，有相關的網站伺服器強化措施及定期執行網站技術弱點處理程序。	皆適用	ISO 27001
6.2 電子郵件安全管理	6.2.1 應對電子郵件程式進行相關安全設定，如需傳送客戶資料或訂單資料宜加密保護。	皆適用	ISO 27001
	6.2.2 應訂定營業用電子郵件帳號申請與密碼訂定之要求，並設定郵件規則防止垃圾郵件與詐騙郵件。	皆適用	ISO 27001
	6.2.3 應限制高風險業務或敏感性資訊避免使用即時通訊軟體或外部電子郵件信箱進行資料傳輸作業。	皆適用	ISO 27001
6.3 個人資訊設備安全管理	6.3.1 應定期進行系統更新，以避免遭受弱點攻擊。	皆適用	ISO 27001
	6.3.2 應制定使用者電腦使用管理規範，要求使用者通行碼、電腦使用、資訊設備操作及工作行為需注意事項。	皆適用	ISO 27001
策略目標：7.建立外部單位資料交換安全管理			

管理項目	要求項目	類別	依據之法規或標準
7.1 配送資料交換協議與保護措施	7.1.1 應與電子商務網路平台、店家或供應商協定電子資料交換機制，並予以保護。	皆適用	ISO 27001
7.2 配送資料傳遞過程儲存媒體的保護	7.2.1 應保護內有客戶資料之實體媒體交換，並採用可靠的傳遞管道。	皆適用	ISO 27001
策略目標：8.建立資安通報管理機制			
8.1 電子商務資安通報機制	8.1.1 應參照電子商務資安通報機制規範，進行資安事故外部通報。	皆適用	ISO 27001
8.2 資安事故管理	8.2.1 應建立資安事件與個資外洩通報程序，並對內外部員工宣導相關通報流程。	皆適用	ISO 27001
	8.2.2 應收集、保存及呈現資安事故之完整證據，並針對事故之原因進行檢討分析。	皆適用	ISO 27001

資料來源：本計畫整理

伍、規範查檢表

說明：

(一) 查檢表格式依循規範大綱及管理項目，分別制定要求之查檢項目與對應之檢核方法

(二) 類別欄位未標示者，表示第一、二類業者皆適用；標示“II”表示僅第二類業者適用。

(三) 進階指引欄位標示“◎”表示為進階指引(Better Practices)之參考項目，可依據風險管理需求選擇性執行；未標示者表示該查檢項目為應執行之作業基準(Baselines)，業者應落實執行。

(四) 檢核結果欄位，提供業者自我查核或第三方查核時，針對該查檢項目之查核結果，記錄執行現況是否符合要求。進階指引項目於查核前，應先辨識該項目是否適用，經辨識為不適用項目者，毋須再做檢核紀錄。

(五) 檢核紀錄欄位，提供業者自我查核或第三方查核時，針對該查檢項目之執行現況予以記錄。該欄位已列出之相關紀錄確認，為提供業者實施本規範之操作面參考，非為執行限制，故檢核紀錄可增列所有實際檢核之佐證資訊。

表 7　規範查檢表

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1. 促進組織資訊安全管理					
1.1 資訊安全框架					
1.1.1 物流商應擬定資安政策，由管理階層具體說明其對資安之承諾與責任，並依據政策落實資安管理。					
1.1.1.1	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)？			□ 適用 □ 不適用 說明：	□ 制定政策，內容包含： - 資訊安全目標

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					- 概要資訊安全原則的需求 - 公司內部權責 ☐ 政策公告內部員工 ☐ 政策公告給外部廠商 ☐ 政策定期審查與更新
1.1.1.2	是否建立資訊安全相關文件及其紀錄之管理與管制程序？	II	◎	☐ 適用 ☐ 不適用 說明：	
1.1.1.3	高階管理階層是否制定、審查及核准資訊安全實作？			☐ 適用 ☐ 不適用 說明：	
1.1.1.4	是否指派適當權責之管理階層或成立跨部門單位負責推動、協調及監督資訊安全管理事項？	II	◎	☐ 適用 ☐ 不適用 說明：	☐ 指派特定管理階層 ☐ 成立跨部門資安小組
1.1.1.5	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？			☐ 適用 ☐ 不適用 說明：	
1.1.1.6	是否定期或當資安作業環境發生重大變更時，召開管理審查會議，獨立審查公司對管理資訊安全的作法與其實作(例如：各項資訊安全的控制目標、控制措施、政策、過程及程序)？	II	◎	☐ 適用 ☐ 不適用 說明：	☐ 定期召開資安管理審查會議並留有會議紀錄 ☐ 召開管理審查會議審查重大變更(如：機房搬遷)
1.1.2 物流商宜訂定資安與個人資料管理之稽核程序，設置稽核人員定期進行內部稽核作業，並於後續進行追蹤與改善。					
1.1.2.1	是否留存處理人員身分鑑別、授權及其行為紀錄以供事後稽查？	II		☐ 適用 ☐ 不適用 說明：	☐ 留存使用者身份登出入紀錄

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					□ 留存存取客戶資料紀錄
1.1.2.2	機密敏感資料檔案之更新、更正或註銷是否均報經核准後執行並詳實記錄執行內容、作業人員及時間？	II		□ 適用 □ 不適用 說明：	
1.1.2.3	是否訂有資訊安全與個人資料管理之稽核程序與設置稽核人員，建立內部稽核計畫(含稽核目標、範圍、時間、程序、人員)，並定期辦理資安與個資管理之內部稽核，並存有稽核紀錄？	II	◎	□ 適用 □ 不適用 說明：	□ 訂有資安內部稽核計畫 □ 定期辦理資安內部稽核
1.1.2.4	內部稽核後是否產生稽核報告並追踪建議事項之改善情形(包括稽核發現的摘要、稽核區域、缺失說明及改進建議等)？	II	◎	□ 適用 □ 不適用 說明：	□ 產生稽核報告 □ 追踪改善情形，留有後續改善紀錄
1.2 資訊資產風險管理					
1.2.1 物流商宜建立適當之資產管理機制，分析其作業流程之資安風險與建立因應對策；並針對核心營運流程中斷之機率及衝擊進行評估，落實必要之營運持續計畫。					
1.2.1.1	若達第二類業者規模，是否遵循「電子商務交易安全規範-網路平台：1.2 風險管理」相關要求？	II		□ 適用 □ 不適用 說明：	
1.2.1.2	若達第二類業者規模，是否參考「電子商務交易安全規範-網路平台：1.3 資訊資產管理」考量適當查檢項目予以落實？	II		□ 適用 □ 不適用 說明：	
1.2.1.3	若達第二類業者規模，是否參考「電子商務交易安全規範-網路平台：2.5 核心營運系統營運持續管理」考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
1.3 人力安全管理					
1.3.1 物流商宜針對相關作業人員之可能偏差行為(如資料盜取或操作錯誤)，預先具體約束與控管。					
1.3.1.1	是否明確定義背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及聘僱相關法令？	II	◎	□ 適用 □ 不適用 說明：	
1.3.1.2	對所有聘僱之應徵者、承包者及第三方使用者的之派任或升任，是否作適當之背景查證檢核？(如：工作職務涉及客戶資訊、通訊內容存取者，則需更進一步的背景查	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	證檢核。)				
1.3.2 物流商應針對相關作業人員進行資安與個人資料保護的教育訓練與宣導。					
1.3.2.1	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？			☐ 適用 ☐ 不適用 說明：	☐ 管理階層以公告或宣導之任何方式要求依程序執行安全事宜 ☐ 告知內部員工 ☐ 告知外部廠商
1.3.2.2	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？			☐ 適用 ☐ 不適用 說明：	☐ 施行資安教育訓練並留存訓練紀錄 ☐ 內部員工參與 ☐ 外部廠商參與
1.3.2.3	是否對處理或保有客戶個人資料之人員施予客戶個人資料保護之教育訓練，並定期於部門內宣導個資隱私保護之重要性？			☐ 適用 ☐ 不適用 說明：	☐ 施行客戶隱私保護相關教育訓練 ☐ 訂定宣導文件並公告公司內部員工與外部廠商
1.3.2.4	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產？(包含歸還所有先前發出的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他公司資產)			☐ 適用 ☐ 不適用 說明：	
1.3.2.5	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？			☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.3.2.6	是否訂有員工違反公司安全政策與程序之懲處規定？	II	◎	☐ 適用 ☐ 不適用 說明：	
1.3.3 物流商應針對相關作業人員之資訊存取權限進行控管。					
1.3.3.1	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？			☐ 適用 ☐ 不適用 說明：	☐ 程式開發與資料庫管理權限予以分散 ☐ 備有權責區分表
1.3.3.2	員工、產業供應鏈上下游業者及任何其他第三方使用者的法定責任與權利是否明確定義且傳達給員工？			☐ 適用 ☐ 不適用 說明：	☐ 訂定並公告資安責任 ☐ 向內部員工公告 ☐ 向外部廠商公告
1.3.3.3	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？			☐ 適用 ☐ 不適用 說明：	☐ 員工已簽署保密協議 ☐ 外部廠商已簽署保密協議
1.3.3.4	是否詳細檢查職務能合法存取關鍵服務、客戶資訊，客戶要求的內容已納入相關安全責任？	II	◎	☐ 適用 ☐ 不適用 說明：	
1.4 遵循性管理					
1.4.1 物流商之資安作為應遵守民法、刑法、消保法、智慧財產權與個資法等相關法令法規，並滿足所提供之服務契約要求。					
1.4.1.1	物流商是否參考「電子商務交易安全規範-網路平台：1.5 遵循性管理」予以落實查檢項目？			☐ 適用 ☐ 不適用 說明：	
1.5 客戶及第三方管理					
1.5.1 於上、下游電子資料交換協同作業中(含資料往返、互換及二次以上傳遞)，應確保作業之資訊安全，並與委外廠商於簽訂合約時訂定保密條款。					
1.5.1.1	是否確保均不違反任何法律、法令、法規或契約義務，以及任何安全要求？			☐ 適用 ☐ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.5.1.2	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？			□ 適用 □ 不適用 說明：	
1.5.1.3	合作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。			□ 適用 □ 不適用 說明：	□ 合作廠商未擁有營運系統或客戶資料之存取權限 □ 合作廠商擁有部分營運系統或客戶資料之存取權限須經正式申請程序
1.5.1.4	合作廠商若有存取系統之行為，是否將記錄重要系統中所有存取及操作的紀錄及其相關儲存規則，列入系統需求規範中？	II		□ 適用 □ 不適用 說明：	
1.5.1.5	當與合作廠商之關係中止時(包括到期自然中止與強制中止) ，是否將申請其所有的實體與系統權限通報取消？			□ 適用 □ 不適用 說明：	□ 終止合約之廠商未有實體與系統權限
1.5.1.6	合作廠商取得有關客戶之敏感資料前，是否由該合作廠商合約之簽訂單位負責過濾，並列入查核重點？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.7	與合作廠商簽訂服務合約之單位，是否同時負責監督委外廠商工作之品質？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.8	合作廠商因負責重要文件及資訊資產相關業務者(包括但不限於客戶消費模式或使用習性分析；為促銷、抽獎等活動所執行之客戶資料收集與後續獎項寄送等活動之儲存、複製、傳遞運送、銷毀等事項)，是否於選商階段或承接業務後接受資訊安全查核單位不定期抽檢，並提供資訊安全查核單位相關資料與報告？	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
1.5.1.9	查核所發現之不符合事項，受查廠商是否回覆處理結果或改進期限以供公司進行後續追蹤？經查核判定情節重大者，應列入受查核廠商立即修正事項；未於限期內完成時，資訊安全查核單位得建議中止其選商資格或暫停其所承接之業務，直到改善完畢後在考量予以恢復。	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.10	因營運需要開放給產業供應鏈(含物流商、金流業者、供應商、其他資訊服務廠商、臨僱人員與消費者等)使用之資訊，是否予以識別，並於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.11	因營運需要開放給外部產業供應鏈或人員存取之資訊，其存取權限是否定期審查？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.12	供應鏈合作或委外契約中有關安全需求內容是否包含法律要求(如個人資料保護法)、雙方有關人員權責、安全控管措施、作業程序、事件通報程序、服務水準、對外部產業供應鏈與委外廠商稽核權等資訊安全責任與事宜，並得依實際需要隨時修改安全控管措施及作業程序等？	II	◎	□ 適用 □ 不適用 說明：	
1.5.1.13	與委外廠商簽訂合約時，內容是否至少包含但不限於下列精神之保密敘述： (1) 對於公司之客戶資料負絕對之保密義務及保管責任，未經本公司同意，絕不以任何方式將其洩露、告知、交付予任何第三人，若有違反以致公司遭受損害，合約廠商應同意無條件賠償本公司所受之一切損害(包括訴訟上及非訴訟上之損害)。 (2) 另如涉有民刑事責任，合約廠商並應負起相關所有民刑事責任。			□ 適用 □ 不適用 說明：	
2.加強核心資訊系統安全管理					
2.1 核心資訊系統取得、開發及維護安全管理					
2.1.1 物流商的新資訊系統或現有資訊系統中，為了保障安全宜考量以文件詳述資訊安全之要求。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1.1.1	物流商若透過委外或自行開發新系統，是否遵循「電子商務交易安全規範-網路平台：2.1.1」相關要求？	II		□ 適用 □ 不適用 說明：	□ 是否備有系統分析文件 □ 是否備有系統設計文件 □ 內容是否至少包含應用系統的流程、架構、初步系統設計、輸出入資料規格、介面設計構想、資料庫架構(Schema)等項目
2.1.2 輸入核心資訊系統的資料應透過程式邏輯設計予以檢查，確保資料正確。					
2.1.2.1	若達第二類業者規模，是否遵循「電子商務交易安全規範-網路平台：2.1.2 」相關要求？	II		□ 適用 □ 不適用 說明：	□ 對字串的輸入加以過濾與限制長度 □ 過濾單、雙引號 □ 針對輸入邏輯進行檢查
2.1.3 核心資訊系統的作業系統之升級或更新應有適當的管制，更新前應進行測試，測試環境宜予以獨立，並避免以真實客戶資料進行。					
2.1.3.1	核心資訊系統之作業系統軟體更新是否需經管理階層授權之人員處理？			□ 適用 □ 不適用 說明：	
2.1.3.2	作業系統若需變更或升級，是否對核心資訊系統作相容性評估？	II		□ 適用 □ 不適用 說明：	□ 先行於測試機器更新進行軟體相容性評估
2.1.3.3	若達第二類業者規模，是否遵循「電子商務交易安全規範-網路平台：2.1.4」相關要求對測試環境應予以獨立，並避免以真實客戶資料進行？	II		□ 適用 □ 不適用 說明：	
2.1.4 核心資訊系統應於新功能上線或變更時執行測試，測試內容應同時考慮系統功能、可用性及安全性。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.1.4.1	是否建立核心資訊系統之變更管制程序？	II	◎	□ 適用 □ 不適用 說明：	
2.1.4.2	核心資訊系統變更前後，是否評估異動範圍、時間、可能之影響？			□ 適用 □ 不適用 說明：	
2.1.4.3	核心資訊系統變更前是否提出於測試系統演練過之緊急復原步驟？			□ 適用 □ 不適用 說明：	□ 提出緊急復原步驟與計畫 □ 事前演練緊急復原步驟
2.1.4.4	核心資訊系統是否維持所有變更紀錄且妥善保存？	II	◎	□ 適用 □ 不適用 說明：	
2.1.4.5	核心資訊系統變更後是否立即更新系統文件？	II	◎	□ 適用 □ 不適用 說明：	
2.1.4.6	委外開發合約中是否規範智慧財產權之歸屬？			□ 適用 □ 不適用 說明：	
2.1.4.7	訂定委外開發合約時是否簽訂安全履行條款與相關罰則？			□ 適用 □ 不適用 說明：	□ 簽訂保密切結與載明保密協議 □ 訂有資安查核或委託第三方查核之權利
2.1.4.8	核心資訊系統上線或變更前的測試作業，是否考量進行相關安全測試項目？	II	◎	□ 適用 □ 不適用 說明：	□ 未開啟不必要的服務與通訊埠 □ 未開啟不必要的通訊協定 □ 未留有不必要的帳號 □ 限制以 URL 直接跳頁瀏覽站內網頁

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					結構 □ 防止程式原始碼與錯誤碼暴露過多資訊 □ 管理員帳號密碼安全程度符合內部規定 □ 輸入欄位已進行測試 □ 已執行防駭測試 □ 已執行弱點掃描
2.1.4.9	是否定期執行各項核心資訊系統之漏洞修補程式？			□ 適用 □ 不適用 說明：	
2.2 核心資訊系統存取控制管理					
2.2.1 核心資訊系統應有足夠強度的帳號密碼申請及管理規定，使用者、系統管理者帳號及權限皆應有申請核准紀錄，及離調職時取消帳號紀錄。					
2.2.1.1	是否設定適當的使用者註冊與取消註冊規定，以對所有核心資訊系統核准和取消其存取權限？			□ 適用 □ 不適用 說明：	
2.2.1.2	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？			□ 適用 □ 不適用 說明：	
2.2.1.3	基於系統管理或特殊作業需要，如需設定特殊權限時(如系統管理者、高權限之管理者)，是否透過正式的授權過程來控制特權的配置？			□ 適用 □ 不適用 說明：	
2.2.1.4	是否維持所有使用者註冊服務、系統，或存取資訊等之正式紀錄？	II	◎	□ 適用 □ 不適用 說明：	
2.2.1.5	核心資訊系統的內部與外部使用者，是否透過帳號與通行密碼登入？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.2.1.6	核心資訊系統使用者是否均有唯一的使用者識別帳號？			□ 適用 □ 不適用 說明：	
2.2.1.7	在任何情形下提供使用者通行密碼之前，是否進行身份確認程序？			□ 適用 □ 不適用 說明：	□ 核對識別證或其餘身份識別 □ 寄至使用者公司郵件信箱或任何電子身份確認方式
2.2.1.8	是否強制要求使用者初次登入電腦或系統後，必須立即更改預設之通行密碼；或於一定期限內未登入，則預設通行密碼將失效，必須重新再申請建立？			□ 適用 □ 不適用 說明：	
2.2.1.9	是否定有使用者通行密碼管理規則，至少規定長度須超過 6 個字元及需混合大小寫字母及數字？			□ 適用 □ 不適用 說明：	
2.2.1.10	是否不允許在登入過程中自動登載使用者通行碼？	II		□ 適用 □ 不適用 說明：	
2.2.1.11	是否規定避免使用與個人有關資訊(如生日、身份證字號、單位簡稱、電話號碼等)當做使用者通行密碼？	II		□ 適用 □ 不適用 說明：	
2.2.1.12	是否避免保留使用者通行密碼的紀錄(例如：紙張、軟體檔案或手持裝置)， 除非其能被安全地存放，且該存放方式經過核准？	II	◎	□ 適用 □ 不適用 說明：	
2.2.1.13	針對連續登入錯誤的鎖定，是否訂定正式的解鎖驗證或重新取得授權程序？	II	◎	□ 適用 □ 不適用 說明：	
2.2.1.14	是否依據核心資訊系統之機敏程度，針對通行密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)？	II		□ 適用 □ 不適用 說明：	
2.2.1.15	是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資訊？	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.2.1.16	是否定期或依規定期限(或使用次數限制)，要求變更使用者通行密碼，並避免重複或循環使用舊有相同之使用者通行密碼？	II		□ 適用 □ 不適用 說明：	
2.2.1.17	是否避免讓輸入之使用者通行密碼以明文方式顯示在螢幕上？			□ 適用 □ 不適用 說明：	
2.2.2 重要作業職權(如處理個資相關作業)應加以區隔，以降低資產遭未經授權或非意圖的修改或誤用之機會。					
2.2.2.1	對於安全要求高的資訊業務(如：牽涉客戶資料)，是否盡可能區隔其職務與責任領域？			□ 適用 □ 不適用 說明：	□ 備有職務分配表
2.2.2.2	核心資訊系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否盡可能授權由不同的人員執行？	II		□ 適用 □ 不適用 說明：	
2.2.3 核心營運系統之公用程式應用(如遠端連線程式、外部連線存取等)應進行管制。					
2.2.3.1	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)？			□ 適用 □ 不適用 說明：	□ 限制遠端連線 □ 限制 telnet 連線 □ 限制 FTP 連線
2.2.3.2	對於核心資訊系統，是否限制網路會談結束或超過界定的未動作時限後，即予中斷連線或關閉設備？	II		□ 適用 □ 不適用 說明：	
2.2.3.3	核心資訊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？	II		□ 適用 □ 不適用 說明：	
2.3 核心資訊系統資料庫安全管理					
2.3.1 核心資訊系統的資料庫應建立連線管制與存取控制機制，以保護消費者資料與交易資訊。					
2.3.1.1	物流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。			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
2.3.1.2	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，並避免周邊存取(USB)行為？			□ 適用 □ 不適用 說明：	
2.3.1.3	應用程式連結帳號是否禁止擁有異動與資料庫相關檔案的作業系統權限？	II	◎	□ 適用 □ 不適用 說明：	
2.3.1.4	應用軟體開發者是否禁止直接連接操作資料庫，或只能使用應用程式連結存取其授權範圍的資料？	II	◎	□ 適用 □ 不適用 說明：	
2.3.1.5	應用系統資料本身之安全性不同，若因涉及公司或個人機密資料所無法對外或對所有維護人員開放查詢，是否由應用程式開發者使用加解密功能對資料庫內其被授權範圍資料進行存取，避免資料庫管理者可直接解讀機密資料?	II	◎	□ 適用 □ 不適用 說明：	
2.3.2 核心資訊系統的資料庫應定期查檢，以保護消費者資料與交易資訊之正確與完整。					
2.3.2.1	資料庫專任管理人員是否每日完成資料庫日常檢核作業表單或紀錄？			□ 適用 □ 不適用 說明：	
2.3.2.2	資料庫日常檢核作業表單是否至少但不限於包含以下項目？(1) Database Information (2) Database Archive/Transaction Log Directory Utilization (3) DB Space and Utilization (4) Check Backup Log (5)Check Database Log (6) Check Session Amount。	II	◎	□ 適用 □ 不適用 說明：	
2.3.2.3	資料庫專任管理人員所屬權責主管，是否每月不定期抽驗資料庫日常檢核作業表單N次以上並簽核存檔，確保紀錄確實性？	II	◎	□ 適用 □ 不適用 說明：	
2.3.24	是否有資料庫遭遇重大問題事件且會影響系統服務之障礙處理流程？	II	◎	□ 適用 □ 不適用 說明：	
2.3.3 核心資訊系統之資料庫應定期備份，並留存重要存取紀錄。					
2.3.3.1	物流商是否參考「電子商務交易安全規範-網路平台：2.4 核心營運系統資料庫安全管理」與「電子商務交易安全規範-網路平台:4.1.4 重要資料及資訊系統應定期進行系統與軟體的備份與還原測試」予以落實	II		□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	查檢項目？				
2.3.3.2	資料庫管理者之操作行為是否記錄？	II		□ 適用 □ 不適用 說明：	
2.3.3.3	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。	II		□ 適用 □ 不適用 說明：	
3.保護客戶個人資料檔案安全					
3.1 客戶資料隱私管理原則					
3.1.1 應於網站或公司營運據點所屬範圍之適當地點公告隱私權保護宣告或政策，相關資訊至少包含客戶資料蒐集與利用範圍、第三方協同作業範圍、資料保護安全措施等。					
3.1.1.1	是否於網站或公司營運據點所屬範圍之適當地點，公告隱私權保護宣告或政策？			□ 適用 □ 不適用 說明：	□ 包含 -客戶資料蒐集與利用範圍 -第三方協同作業範圍 -資料保護安全措施
3.1.2 宜依相關法令指定專人辦理安全維護及客戶個人資料保管事項，且設置對外公告「客戶個人資料保護聯絡窗口」，協調聯繫客戶資料事宜，及擔任消費者提出申訴與救濟時之單一窗口。					
3.1.2.1	處理客戶個人資料之部門，是否指定專人依相關法令辦理安全維護及客戶個人資料保管事項？			□ 適用 □ 不適用 說明：	
3.1.2.2	是否設置「客戶個人資料保護聯絡窗口」，協調聯繫客戶資料事宜，並將聯繫方式(如：電話、E-mail)置於公司網站，以便利消費者提出申訴與救濟？	II		□ 適用 □ 不適用 說明：	
3.1.2.3	是否依據「個人資料保護管理規範」各項要求定期執行自我評量，並培訓內部隱私標章管理人員？	II	◎	□ 適用 □ 不適用 說明：	
3.1.3 應定期盤點物流業務所涉及的客戶個人資料之敏感等級、儲存使用方式、傳輸媒介、接觸人員等，並評估其可能遭遇的重大風險，建置相對應的安全維護措施強度。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.1.3.1	是否瞭解、定義與記錄保有客戶個人資料之相關風險？			□ 適用 □ 不適用 說明：	
3.1.3.2	物流商是否參考「電子商務交易安全規範-網路平台：3.2 客戶資料盤點作業」予以落實查檢項目？	II	◎	□ 適用 □ 不適用 說明：	
3.2 客戶資料依法對外公開、資訊揭露作業					
3.2.1 應依據法律規定、契約及正式對外宣告之隱私權政策，並於蒐集時即告知客戶相關訊息，始得執行客戶個人資料對外公開、資訊揭露等作業。					
3.2.1.1	若必須公開或揭露客戶個人資料給第三方單位，公司是否已檢查揭露客戶個人資料給第三方之作業依據法令並取得客戶同意？			□ 適用 □ 不適用 說明：	
3.2.1.2	若客戶個人資料需公開或揭露給第三方單位，是否確保第三方可提出其存取個人資料之權利或法令依據？並於必要時提出其第三方身分識別資料？	II		□ 適用 □ 不適用 說明：	
3.2.1.3	若必須公開或揭露客戶個人資料給第三方單位，是否經過檢查手續，確保僅揭露最少數量之客戶個人資料項目給第三方？			□ 適用 □ 不適用 說明：	
3.2.1.4	若必須公開或揭露客戶個人資料給第三方單位，是否留存相關作業紀錄並確保可查詢到客戶同意或法令之依據？	II	◎	□ 適用 □ 不適用 說明：	
3.2.1.5	若需於公司管理之網站或網頁公布個人資料時，是否經所屬部門主管核准，並依相關法律及規範處理？	II	◎	□ 適用 □ 不適用 說明：	
3.2.2 宜訂定包含所有線上及離線作業之客戶個人資料保護相關程序，規定客戶資料對外公開、資訊揭露作業之期間、地區、對象、處理方式與保護範圍(界定交易網頁由平台業者或委外第三方單位控管)。					
3.2.2.1	是否訂定客戶個人資料保護之程序與政策？	II	◎	□ 適用 □ 不適用 說明：	□ 包含規範客戶資料對外公開、資訊揭露作業之期間、地區、對象、處理方式與保護範圍(界定交易網

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
					頁由平台業者或委外第三方單位控管)
3.3 客戶資料取得、處理、儲存及其機密性與正確性管理					
3.3.1 取得、處理或利用客戶個人資料時，應依照法令規定及契約要求，透過文字描述其合理關連之特定目的、使用方式及消費者個人資料相關權利之行使方式，並取得當事人同意；變更使用目的或方式時亦需重新取得同意。					
3.3.1.1	蒐集、處理或利用客戶個人資料時，是否透過文字描述其合理關連之特定目的，並經當事人書面同意？			□ 適用 □ 不適用 說明：	□ 說明特定目的 □ 取得書面同意
3.3.1.2	向當事人蒐集客戶個人資料時，是否明確告知消費者蒐集個人資料之目的、類別、利用期間、地區、揭露對象及方式？			□ 適用 □ 不適用 說明：	
3.3.1.3	所獲得之個人資料時，是否確認蒐集者已明確告知當事人以下得行使之權利及方式並取得同意？(1)查詢或請求閱覽。(2)請求製給複製本。(3)請求補充或更正。(4)請求停止蒐集、處理或利用。(5)請求刪除。	II		□ 適用 □ 不適用 說明：	□ 蒐集來源存有當事人同意之佐證資料
3.3.1.4	客戶相關個人資料不得提供非該次交易必要範圍外之使用；如需變更資料利用之目的，是否重新以書面取得當事人之同意？			□ 適用 □ 不適用 說明：	
3.3.2 客戶個人資料之處理行為應經權責單位核准，並對處理客戶資料人員存取權限進行控管。					
3.3.2.1	客戶個人資料之處理行為是否經權責單位核准？			□ 適用 □ 不適用 說明：	
3.3.2.2	處理客戶個人資料檔案之人員職務異動時，是否依規定列冊移交相關媒體及資料？接替人員是否於相關系統重置密碼，並視需要更換使用者帳號？	II	◎	□ 適用 □ 不適用 說明：	
3.3.2.3	處理客戶個人資料檔案之人員，是否簽訂保密切結書？			□ 適用 □ 不適用 說明：	
3.3.2.4	處理客戶個人資料檔案之人員離職時，是否依規定取消或停用其使用者識別帳號並收繳通行證件？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.3.2.5	客戶個人資料之輸出入與處理個人資料檔案之個人電腦，是否均以帳號密碼管制？			□ 適用 □ 不適用 說明：	
3.3.3 應對客戶提出其個人資料查詢、更新與申訴等服務時，有完整的執行步驟與客戶回應說明。如客戶欲維護個人資料之正確性或發生爭議時，尊重消費者權益與意願，立即停止處理或利用，並於 30 日內予以回應處理狀況。					
3.3.3.1	是否制定程序，在必要時及時更新客戶個人資料？	II		□ 適用 □ 不適用 說明：	□ 定期提醒客戶更新資料 □ 配合客戶需求更新資料
3.3.3.2	是否制定關於客戶個人資料諮詢與申訴的相關處理程序？			□ 適用 □ 不適用 說明：	□ 備有客戶個資處理之標準作業程序
3.3.3.3	消費者欲維護個人資料之正確性時，是否有相關之程序主動或供當事人申請更正或補充，並於 30 日內予以回應？	II		□ 適用 □ 不適用 說明：	
3.3.3.4	客戶個人資料正確性發生爭議時，是否有相關之程序主動或供消費者申請停止處理或利用，並於 30 日內予以回應？	II		□ 適用 □ 不適用 說明：	
3.3.4 利用電腦處理客戶個人資料時，應有內部作業查驗程序，以確保輸入資料與原資料相符合。					
3.3.4.1	利用電腦處理客戶個人資料時，是否有相關查驗程序確保輸入資料與原資料相符合？	II		□ 適用 □ 不適用 說明：	□ 備有資料輸入抽核機制
3.4 客戶資料使用及傳輸安全作業					
3.4.1 物流客戶個人資料之使用、傳遞與交換作業，應有加密或其他適當保全機制，並明確規定執行作業之期間、地區、對象、申請及處理方式。					
3.4.1.1	因業務需求，欲遞送客戶個人資料給予內部其他負責單位時或回收紙本資料時，是否將使用專用信封並密封？			□ 適用 □ 不適用 說明：	
3.4.1.2	因業務需求交換電子客戶個人資料給予公司內部其他單位負責人員處理時，是否將檔案加密？	II		□ 適用 □ 不適用 說明：	
3.4.1.3	交換紙本客戶個人資料時，是否採取彌封或其他具備保密機制之傳遞方式？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.4.1.4	如需傳遞或複製客戶資料給予第三者時，是否確認此外部第三者已與公司簽訂載明雙方權利義務之保密協議書或相關且有法律效力之安全文件？			□ 適用 □ 不適用 說明：	□ 訂定保密協議
3.4.1.5	與外部廠商或人員以電子遞送方式交換客戶資料時，是否採取可靠且具備保密機制之傳遞方式？	II		□ 適用 □ 不適用 說明：	□ 檔案加密 □ 透過專屬安全連線與帳號、通行密碼
3.4.1.6	交換及調閱個人資料等作業，是否記錄並保存作業人員之身分及行為，紀錄中包含轉交或傳輸行為之流向？	II	◎	□ 適用 □ 不適用 說明：	
3.4.1.7	任何含有客戶資料的文件或電子媒體，其複製行為是否在規劃的伺服器或安全磁碟區中執行？	II	◎	□ 適用 □ 不適用 說明：	
3.4.1.8	客戶資料之查詢存取，是否使用雙重識別認證(如：生日+身分證字號或行動電話號碼+取件地點)的方式為之？	II		□ 適用 □ 不適用 說明：	
3.4.1.9	是否針對客戶個人資料檔案之列印進行記錄？			□ 適用 □ 不適用 說明：	
3.4.1.10	針對客戶個人資料相關系統規劃及設計之協力廠商，是否由系統負責部門控管該協力廠商之閱讀及印製權限，並查核系統使用紀錄？	II	◎	□ 適用 □ 不適用 說明：	
3.4.1.11	是否禁止使用 MSN 或其他即時通訊軟體、外部網頁式電子郵件(Webmail)傳輸客戶個人資料檔案，並禁止安裝點對點(P2P)軟體及 Tunnel 相關工具避免客戶個人資料檔案外流？	II		□ 適用 □ 不適用 說明：	□ 限制 MSN 傳輸檔案 □ 限制 P2P 傳輸 □ 限制使用外部網頁式電子郵件
3.5 客戶資料刪除及停止利用作業					
3.5.1 含有客戶資料之儲存媒體，淘汰報廢時，應使用格式化或其他實體破壞方式予以銷毀。					
3.5.1.1	儲存客戶個人資料檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其所儲存之客戶個人資料檔案？			□ 適用 □ 不適用 說明：	□ 刪除客戶資料 □ 進行格式化 □ 實體破壞儲存媒體

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
3.5.2 應控管配送作業相關客戶個人資料留存的時間，定期由專人或負責人員刪除，並由主管不定期抽檢。					
3.5.2.1	是否控管客戶個人資料留存的時間，定期由專人或負責人員刪除，並由主管不定期抽檢？			☐ 適用 ☐ 不適用 說明：	
3.5.2.2	各項電子形式之客戶資料報表，是否於完成處理作業後，應由各負責單位於報表保存期限到期前，進行檔案之刪除作業？	II	◎	☐ 適用 ☐ 不適用 說明：	
4.加強託運單安全管理					
4.1 託運單資料管理					
4.1.1 客戶託運單應避免出現完整之客戶資訊，並對電子託運資料進行保護與備份。					
4.1.1.1	客戶託運單是否針對除交遞必須之資訊予以適當遮隱，避免出現完整之客戶身分証號、所託運之貨品詳細內容、各種金流交易資訊，與發票相關資料等，以確保客戶隱私?			☐ 適用 ☐ 不適用 說明：	
4.1.1.2	處理中的客戶物流資料是否定期作備份處理？			☐ 適用 ☐ 不適用 說明：	
4.1.1.3	作業環境之電腦，是否不儲存業務目的消失後超過一週以上之客戶託運資料？			☐ 適用 ☐ 不適用 說明：	☐ 未存有一週以上之客戶資料
4.1.1.4	作業環境之電腦，若留存一週以上且非日常業務頻繁使用之客戶託運資料，是否以密碼加密？			☐ 適用 ☐ 不適用 說明：	☐ 加密客戶資料 ☐ 存於加密磁區
4.1.1.5	業務目的消失後一週以上之客戶託運資料，是否集中控管於權限控管之公用資料夾，並依業務需求定期刪除？			☐ 適用 ☐ 不適用 說明：	☐ 集中控管並設定適當權限 ☐ 定期檢視作業需求並刪除客戶資料
4.1.1.6	託運單掃描電子檔資料是否每月備份為光碟存檔，並由專人上鎖保管？	II		☐ 適用 ☐ 不適用 說明：	
4.2 紙本託運單之保存及銷毀管理					
4.2.1 紙本託運單應集中保存，並僅限授權人員使用或進出集中保管處。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.2.1.1	託運單處理作業相關人員於作業中離開座位或下班時，是否妥善收存紙本託運單並鎖定電腦避免處理中之託運資料外洩？			□ 適用 □ 不適用 說明：	
4.2.1.2	是否每日檢查作業環境周遭是否有未妥善保管之託運單？			□ 適用 □ 不適用 說明：	
4.2.1.3	當週需應用於查詢之紙本託運單，是否集中於上鎖鐵櫃，並由專人控管鑰匙？			□ 適用 □ 不適用 說明：	□ 集中控管並妥善上鎖存管 □ 鑰匙由專人負責保管
4.2.1.4	當週紙本託運單之調閱是否僅限現場作業之授權人員？			□ 適用 □ 不適用 說明：	□ 僅授權適當人員調閱託運單
4.2.1.5	是否將留存一週以上之紙本託運單集中保管於託運單庫房或有門鎖之集中保管場所？	II		□ 適用 □ 不適用 說明：	□ 留存一週以上紙本託運單集中保管
4.2.1.6	庫房環境是否控制適當溼度，若發現溼度超出一定濕度時則進行除濕，並且每星期將溼度檢查紀錄於表單？			□ 適用 □ 不適用 說明：	□ 濕度檢查紀錄記載於表單 □ 濕度超限時立即除濕
4.2.1.7	授權人員方可進入託運單庫房，非授權人員進出託運單庫房時是否於託運單庫房管制表註明？			□ 適用 □ 不適用 說明：	□ 僅授權適當人員進出託運單庫房
4.2.1.8	庫房是否置放非灑水式之適當消防設備，並定期檢測？	II		□ 適用 □ 不適用 說明：	
4.2.1.9	託運單是否依法令法規要求保存至少五年之年限？	II		□ 適用 □ 不適用 說明：	
4.2.2 準備丟棄作廢或不再持有之託運單或客戶配送單與簽收單等紙本資料，應使用碎紙機或其他實體破壞方式予以確實銷毀，或委由專業處理廠商於專人監督下銷毀。					
4.2.2.1	少量無需歸檔或廢棄內含客戶資料之託運單，是否使用碎紙機銷毀？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.2.2.2	託運單銷毀作業是否有清點及確認作業紀錄？	II		□ 適用 □ 不適用 說明：	
4.2.2.3	託運單保存之年限屆滿時，是否有相關之程序主動刪除或銷毀託運紙本與電子資料？			□ 適用 □ 不適用 說明：	
4.2.2.4	託運資料銷毀承辦人員是否向部門主管提出申請核備？於核可後方得辦理銷毀。	II	◎	□ 適用 □ 不適用 說明：	
4.2.2.5	大量之機敏文件銷毀是否統一分配裝箱並黏貼封條？	II		□ 適用 □ 不適用 說明：	
4.2.2.6	紙本託運單銷毀方式是否採用水銷處理法、焚毀等確實銷毀紙本資料之方法？	II		□ 適用 □ 不適用 說明：	
4.2.2.7	由廠商協助銷毀時，是否指派監督人員跟隨，並予以拍照並在其監督下進行銷毀？	II		□ 適用 □ 不適用 說明：	
4.2.2.8	銷毀過程中是否全程錄影且監控整個作業流程，以確保無任何個資外洩之可能性？	II	◎	□ 適用 □ 不適用 說明：	
4.2.2.9	是否保留銷毀作業之收件紀錄及銷毀場之銷毀證明至少 N 年存查？	II	◎	□ 適用 □ 不適用 說明：	
4.3 託運單調閱與印製作業管理					
4.3.1 託運單調閱應經過申請與授權，並限制託運單列印電腦環境。					
4.3.1.1	託運單之調閱是否填寫託運單紙本調閱申請表方得調閱？			□ 適用 □ 不適用 說明：	□ 經申請與核准方可調閱託運單
4.3.1.2	託運單紙本調閱表單是否由資安管理權責單位控管借出與交回，且需於託運單交回後再行簽章確認？	II		□ 適用 □ 不適用 說明：	□ 託運單調閱由權責單位統一控管 □ 託運單交回後經檢視並簽屬確認

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
4.3.1.3	客服部門等相關定期調閱單位是否每日以報表控管調閱單據，且經主管核章後歸檔？	II		□ 適用 □ 不適用 說明：	□ 單位定期調閱紀錄以報表控管並經主管核閱
4.3.1.4	是否指定專人限制於特定電腦才可進行宅配單列印作業？			□ 適用 □ 不適用 說明：	□ 留存一週以上紙本託運單集中保管
4.3.1.5	託運單列印電腦是否與網際網路隔離？			□ 適用 □ 不適用 說明：	
4.3.1.6	是否將當日託運單檔案自列印電腦中刪除？			□ 適用 □ 不適用 說明：	
5.加強作業環境安全管理					
5.1 作業與辦公環境安全管理					
5.1.1 應確保作業與辦公場所、託運單儲存及電腦設備機房區域之安全，避免竊盜或損害。					
5.1.1.1	是否對於處理託運資料相關之辦公場所、託運單庫房、電腦設備機房等重要場所劃分管制區域，出入口是否均有門鎖或門禁措施？			□ 適用 □ 不適用 說明：	□ 劃分作業區域並輔以適當支出入管制
5.1.1.2	管制區域內外窗戶、圍籬或大門是否以可上鎖或以其他符合安全之替代方法加以管理，並由管理或保全人員控管鑰匙之領用？			□ 適用 □ 不適用 說明：	□ 管制區域使用適當之管控措施 □ 進出使用之管控媒介(如鑰匙或磁卡等)由專人負責保管
5.1.1.3	是否配置員工或外聘保全公司負責管制區域之保全工作？	II		□ 適用 □ 不適用 說明：	
5.1.1.4	管制區域內電子商務相關作業員工是否易於辨識身份(如：配戴識別證或穿著制服)？			□ 適用 □ 不適用 說明：	
5.1.1.5	是否建置適當管控員工識別證之核發及收回機制？	II		□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.1.1.6	訪客或委外廠商進出管制區域是否需進行登記並由接洽人員陪同進出，並佩戴明顯之臨時識別證？			□ 適用 □ 不適用 說明：	□ 訂定外部人員進入管制區域之方 □ 依律訂方式執行管制區域外部人員管制
5.1.1.7	對存放客戶個人資料檔案之主機、週邊設備及相關設施等，是否置放於實體安全區域？	II		□ 適用 □ 不適用 說明：	□ 置於門禁控管之辦公區域、機房
5.1.1.8	儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，是否指定專人管理並有獨立存放空間(如：鐵櫃或建置門禁管制)與上鎖保管？	II	◎	□ 適用 □ 不適用 說明：	□ 指定專人保管 □ 置於上鎖之鐵櫃
5.1.1.9	儲存個人資料檔案之媒體是否有攜出、拷貝或複製的管控機制，並留存紀錄？	II		□ 適用 □ 不適用 說明：	
5.1.1.10	是否針對管制區域裝設監視錄影設備？	II		□ 適用 □ 不適用 說明：	□ 管制區域架設監視錄影設備 □ 錄影監控檔案定期檢視並備份
5.1.1.11	若裝設錄影監控設備，是否保留一週以上的錄影紀錄？	II		□ 適用 □ 不適用 說明：	
5.1.1.12	管制區域內是否置放滅火器或裝置適當滅火設備？			□ 適用 □ 不適用 說明：	
5.1.1.13	是否訂有核發、收回及更換進出裝置(例如：鑰匙、門禁卡等)之程序及文件紀錄？	II	◎	□ 適用 □ 不適用 說明：	
5.1.1.14	是否對於未經授權進入管制區域及非法侵入事件須訂有通報之程序？	II	◎	□ 適用 □ 不適用 說明：	□ 訂有通報程序 □ 依程序執行並記錄
5.1.2 除機房與辦公區域外，如倉儲站所等配送資料處理地點之設備應設計安全措施，保護場所管控外設備之安全。					

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.1.2.1	是否利用警報系統或監視錄影設備監控處理託運資料相關之重要出入口，防止未經許可人員進出貨物處理及倉儲區域，避免未經許可人員接觸貨物上之客戶資訊及電腦設備？			□ 適用 □ 不適用 說明：	□ 僅授權適當人員進出敏感區域 □ 利用警報系統或監視錄影實施監控
5.1.2.2	無人看管之營業用電腦或網路設備(如：網路集線器)是否上鎖並定期檢查？			□ 適用 □ 不適用 說明：	□ 予以上鎖 □ 定期檢查
5.1.2.3	倉儲站作業用電腦設備是否訂有保護措施，如：使用授權管理、設通行密碼、檔案加密、專人看管？			□ 適用 □ 不適用 說明：	
5.2 營業用電腦設備環境與設備安全管理					
5.2.1 應設計安全措施，確保營業用電腦伺服器與網路設備之安全，避免竊盜或損害。					
5.2.1.1	置放電腦伺服器與網路設備置之機房，是否僅限受允許之員工進出？			□ 適用 □ 不適用 說明：	□ 僅授權適當人員進出機房
5.2.1.2	電腦伺服器與網路設備是否置放於機櫃或桌上？			□ 適用 □ 不適用 說明：	
5.2.1.3	電信纜線(telecommunications lines)、網路佈纜(network cabling)及電源纜線是否有置於塑膠管線保護等隔離保護，以防止互相干擾？	II	◎	□ 適用 □ 不適用 說明：	
5.2.1.4	電腦伺服器與網路設備是否有足夠的通風或冷氣等空調設備？			□ 適用 □ 不適用 說明：	
5.2.1.5	是否備有溫、濕度計，定時登記監控溫度與濕度？	II		□ 適用 □ 不適用 說明：	
5.2.1.6	核心營運系統關鍵設施是否備有 UPS 不斷電系統？	II		□ 適用 □ 不適用 說明：	
5.2.1.7	核心營運系統關鍵設施是否有接地設施、以及足夠電力保護(如：雙 Power 設計)？	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
5.2.1.8	備援電源(如：發電機)是否定期檢查並測試，確保能在斷電期間運作？	II	◎	□ 適用 □ 不適用 說明：	
5.2.1.9	是否具備環控設備，以自動機制掌握電腦與網路設備之環境狀況？	II	◎	□ 適用 □ 不適用 說明：	
5.2.1.10	設備是否依據供應者建議的保養間隔與規格來定期維護檢查，並留下保養紀錄？	II		□ 適用 □ 不適用 說明：	
5.2.1.11	設備之維護與修理是否僅由授權之維護人員執行？	II		□ 適用 □ 不適用 說明：	
5.2.1.12	如採自建機房維運核心營運系統或建置於委外機房，是否參考「電子商務交易安全規範-網路平台：2.3.核心營運系統機房與作業環境實體安全」考量適當查檢項目進行落實？	II	◎	□ 適用 □ 不適用 說明：	
5.2.2 設備外送或淘汰前應進行安全措施，防止資訊外洩。					
5.2.2.1	相關電腦設備或儲存媒體異動或遞送時，是否定有相關的程序進行管理？	II	◎	□ 適用 □ 不適用 說明：	□ 訂有媒體管理程序 □ 依程序執行並記錄
5.2.2.2	人員攜帶電腦設備與媒體進出管制區域時，是否記錄於表單？	II		□ 適用 □ 不適用 說明：	
5.2.2.3	電腦設備送修時，若非屬儲存媒體(如：硬碟)損壞，於送修前是否先取出儲存媒體，不得一起送修？			□ 適用 □ 不適用 說明：	
5.2.2.4	儲存媒體送修時，若內含客戶資料或機敏資訊時，是否先進行備份，存放於安全區域，並刪除送修設備上之資料防止外洩？			□ 適用 □ 不適用 說明：	
5.2.2.5	硬體類設備報廢時，是否由保管單位刪除或格式化所報廢設備內之資料？			□ 適用 □ 不適用 說明：	
5.2.2.6	硬體類設備由廠商協助銷毀時，是否由保管單位指派監督人員在其監督下進行銷毀？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
6.加強網路安全管理					
6.1 網路通訊與資訊作業安全管理					
6.1.1 營業用電腦設備應安裝防毒軟體，並定期更新病毒碼及執行系統掃描作業。					
6.1.1.1	是否每月對電腦系統及資料儲存媒體進行病毒與後門程式掃描？			□ 適用 □ 不適用 說明：	
6.1.1.2	電腦內是否安裝合法防毒軟體，並即時更新最新之病毒碼與掃描引擎？			□ 適用 □ 不適用 說明：	□ 安裝防毒軟體 □ 每日更新 □ 每三日更新
6.1.1.3	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？	II		□ 適用 □ 不適用 說明：	
6.1.1.4	防毒系統管理人員，是否每月彙整防毒系統統計報表，呈核直屬主管？	II	◎	□ 適用 □ 不適用 說明：	
6.1.1.5	防毒系統管理人員處理重大病毒感染事件後(如：一定數量之群聚感染)，是否針對事件處理撰寫報告並研擬後續防禦措施，呈核直屬主管？	II	◎	□ 適用 □ 不適用 說明：	
6.1.1.6	使用者或訪客因業務需求，攜入非公司之資訊設備及媒體時，資訊設備是否於協請防毒系統管理人員安裝防毒軟體、最新修補程式後，才可與網路連接？	II	◎	□ 適用 □ 不適用 說明：	
6.1.1.7	防毒系統管理人員是否配合電子郵件系統與服務，建置電子郵件防毒閘道與安裝郵件伺服器防毒軟體？	II	◎	□ 適用 □ 不適用 說明：	
6.1.2 應定期進行營業用資訊系統與軟體的備份與還原測試。					
6.1.2.1	是否每週針對營業用資訊系統與軟體進行備份？			□ 適用 □ 不適用 說明：	
6.1.2.2	備份是否儲存於遠端地點？距離是否足以避免機房與主要辦公地點發生災難時遭波及？	II	◎	□ 適用 □ 不適用 說明：	
6.1.2.3	備份資訊是否給予適切等級的實體與環境保護，並與機房與辦公主要場地使用的標準一致？(機房與辦公主要場地採用的控	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	制措施可延伸至涵蓋備份作業場地)				
6.1.3 應定期檢測網路安全及對外客戶託運資訊查詢網站之頻寬，以確保網路系統安全與連線品質。					
6.1.3.1	是否定期檢測網路運作環境之安全漏洞？	II		□ 適用 □ 不適用 說明：	
6.1.3.2	是否監控對外客戶查詢網站之流量是否到達頻寬上限，確保服務連線品質及可用性，以提供最佳服務？	II		□ 適用 □ 不適用 說明：	
6.1.3.3	通訊設備是否具備偵測網路壅塞並避免網路壅塞時通訊集中之機制？	II	◎	□ 適用 □ 不適用 說明：	
6.1.3.4	託管之營業資訊系統，是否已定義一旦發生斷線時如何處置的協議或合約？	II	◎	□ 適用 □ 不適用 說明：	
6.1.3.5	若自行建置網路基礎設施達一定規模，是否參考「電子商務交易安全規範-網路平台：4.1 網路通訊與資訊作業安全管理」考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
6.1.3.6	若自建電子郵件伺服器，是否參考「電子商務郵件安全機制控制項」，考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
6.1.4 營業用電腦伺服器應安裝防火牆或入侵偵測系統，定期檢查防火牆和路由器的規則設定，以保護系統之安全。					
6.1.4.1	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？	II		□ 適用 □ 不適用 說明：	
6.1.4.2	防火牆管理員是否限制在指定 IP 與特定連接埠才能登入管理？	II		□ 適用 □ 不適用 說明：	
6.1.4.3	是否將對外提供公開服務之主機群，建置於 DMZ 並保留連線紀錄？	II		□ 適用 □ 不適用 說明：	
6.1.4.4	公司對外傳輸保護措施，是否於網路閘道端安裝過濾設備(如：傳輸內容含機敏資料將會被擷取下來，以提供稽核及主管確認	II	◎	□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	及處理。)?				
6.1.4.5	公司內若運用超過 50 台以上執行物流營業之個人電腦(含移動式電腦)，是否考量採用統一之網域管理機制，並設定適當之帳號管理與安全控制機制？	II	◎	□ 適用 □ 不適用 說明：	
6.1.4.6	若物流商自行建置網路基礎設施達一定規模，網路安全管理、網路服務監控與測試、防範惡意碼與行動碼等項目，是否參考「電子商務安全偵測機制控制項」，考量適當查檢項目予以落實？	II	◎	□ 適用 □ 不適用 說明：	
6.1.5 宜記錄使用者活動、異常及資訊安全事件，保留一段議定期間，以協助未來的調查與存取控制監視。					
6.1.5.1	是否啟用營業用電腦之系統事件日誌，記錄內容應至少包括使用者識別碼、登入登出之日期時間、電腦的識別資訊或其網址？	II		□ 適用 □ 不適用 說明：	
6.1.5.2	存錄設施與日誌資訊是否規劃適當之儲存媒體容量，以避免無法記錄事件或覆蓋以往所記錄事件？	II		□ 適用 □ 不適用 說明：	
6.1.5.3	是否定期審查各項系統事件日誌？	II	◎	□ 適用 □ 不適用 說明：	
6.1.5.4	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？	II	◎	□ 適用 □ 不適用 說明：	□ 日誌審查紀錄
6.1.6 所有交易相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。					
6.1.6.1	所有系統或監視器之日期與時間設定是否每週核對校正以確保時間紀錄正確？	II		□ 適用 □ 不適用 說明：	
6.1.7 宜對公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，有相關的網站伺服器強化措施及定期執行網站技術弱點處理程序。					
6.1.7.1	若公司擁有或委外維運之對外公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，是否參考「電子商務交易安全規範-網路平台：5.3 交易網站伺服器強固」考量適當查檢項目予以落實？	II		□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
6.1.7.2	若公司擁有或委外維運之對外公開網站、對外客戶託運資訊查詢網站或與上下游協同作業介接之網站系統，是否參考，「電子商務交易安全規範-網路平台：5.4 交易網站技術弱點管理」考量適當查檢項目予以落實？	II		□ 適用 □ 不適用 說明：	
6.2 電子郵件安全管理					
6.2.1 應對電子郵件程式進行相關安全設定，如需傳送客戶資料或訂單資料宜加密保護。					
6.2.1.1	敏感或機密性之客戶個資或交易資料，如需以電子郵件附件方式對外傳送，是否採用合宜的加密措施(如：壓縮軟體 RAR、ZIP 加上密碼等)處理後傳送？			□ 適用 □ 不適用 說明：	
6.2.1.2	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？			□ 適用 □ 不適用 說明：	
6.2.1.3	是否關閉電腦端郵件收發軟體(如：Outlook 或 Outlook Express)與 Webmail 的信件自動下載圖片(或其他內容)功能？			□ 適用 □ 不適用 說明：	
6.2.1.4	若使用電腦端郵件收發軟體(如：Outlook 或 Outlook Express)，是否關閉郵件預覽功能？			□ 適用 □ 不適用 說明：	
6.2.1.5	若使用電腦端郵件收發軟體(如：Outlook 或 Outlook Express)，是否使用純文字模式開啟郵件？			□ 適用 □ 不適用 說明：	
6.2.1.6	使用者是否了解電子郵件社交工程威脅？			□ 適用 □ 不適用 說明：	□ 防範社交工程詐騙宣導說明
6.2.1.7	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？			□ 適用 □ 不適用 說明：	
6.2.2 應訂定營業用電子郵件帳號申請與密碼訂定之要求，並設定郵件規則防止垃圾郵件與詐騙郵件。					
6.2.2.1	是否經由填寫申請表單才配給營業用電子郵件信箱？	II		□ 適用 □ 不適用 說明：	
6.2.2.2	是否每季定期更改營業用電子郵件之登入密碼以防止被盜用？			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
6.2.2.3	營業用電子郵件信箱之使用者登入密碼，是否設定至少 6 碼以上？			□ 適用 □ 不適用 說明：	
6.2.2.4	是否取消自動密碼記憶功能，以避免郵件密碼遭擷取？			□ 適用 □ 不適用 說明：	
6.2.2.5	是否設定垃圾郵件過濾機制？			□ 適用 □ 不適用 說明：	
6.2.2.6	是否設定郵件規則，將常往來、熟悉的客戶與廠商設定分類，以防範來路不明或詐騙郵件？	II		□ 適用 □ 不適用 說明：	□ 設定郵件過濾規則
6.2.2.7	電子郵件系統如需發送郵件到公司以外之網域，是否考量於郵件本文後加註隱私權、法律責任聲明等，以保障公司權益？	II	◎	□ 適用 □ 不適用 說明：	
6.2.3 應限制高風險業務或敏感性資訊避免使用即時通訊軟體或外部電子郵件信箱進行資料傳輸作業。					
6.2.3.1	是否考量限制即時通訊相關軟體(如 MSN, Yahoo 即時通, Google talk)之使用？或監控其紀錄與限制傳檔功能？	II	◎	□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
6.2.3.2	是否考量限制公司外部之電子郵件信箱或 Webmail 之使用？或監控其記錄與限制傳檔功能？	II	◎	□ 適用 □ 不適用 說明：	□ 限制使用 □ 限制檔案傳輸 □ 留存監控紀錄
6.3 個人資訊設備安全管理					
6.3.1 應定期進行系統更新，以避免遭受弱點攻擊。					
6.3.1.1	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？			□ 適用 □ 不適用 說明：	□ 作業系統更新是否一致 □ 更新時程≦1個月
6.3.2 應制定使用者電腦使用管理規範，要求使用者通行碼、電腦使用、資訊設備操作及工作行為需注意事項。					
6.3.2.1	營業用個人電腦(含移動式電腦)作業系統與相關應用程式之使用者登入密碼，是否設定至少 6 碼以上？並至少六個月變更一			□ 適用 □ 不適用 說明：	

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
	次？				
6.3.2.2	下班時是否登出電腦系統並關閉電源？			□ 適用 □ 不適用 說明：	
6.3.2.3	機房用機、值班用機或是程式執行之限制需常態開機之電腦，是否每日重新開機，以利開機時完成相關修補程式及病毒碼之更新作業，同時避免電腦遭未經授權的存取？	II	◎	□ 適用 □ 不適用 說明：	
6.3.2.4	是否考量資料安全性，針對桌上型電腦的USB 連接埠停用大量儲存媒體裝置與軟碟機之使用功能？	II	◎	□ 適用 □ 不適用 說明：	
6.3.2.5	包含敏感或機密資訊的文件是否立即從印表機或傳真機上取走？			□ 適用 □ 不適用 說明：	
6.3.2.6	是否設定作業系統內建之螢幕保護程式，以確保公司資料之安全性？			□ 適用 □ 不適用 說明：	□ 螢幕保護程式設定≦15分鐘並以密碼保護
6.3.2.7	下班後經辦之機密性及敏感性資訊或文件是否妥為收存？			□ 適用 □ 不適用 說明：	
6.3.2.8	是否考量限制將未經授權允許之資訊設備、軟硬體攜入辦公場所使用？	II	◎	□ 適用 □ 不適用 說明：	
6.3.2.9	非公司配發及採購之週邊設備，是否考量禁止擅自安裝於內部電腦上？	II	◎	□ 適用 □ 不適用 說明：	
7.建立外部單位資料交換安全管理					
7.1 配送資料交換協議與保護措施					
7.1.1 應與電子商務網路平台、店家或供應商協定電子資料交換機制，並予以保護。					
7.1.1.1	員工是否瞭解電子商務網路平台發放加密憑證之用途，並書面規定憑證安全與管理程序？	II	◎	□ 適用 □ 不適用 說明：	□ 備有書面規定 □ 未違反書面規定

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
7.1.1.2	物流商的資訊設備(如：主機、個人電腦等)與電子商務網路平台之系統連線通道，是否予以加密？			□ 適用 □ 不適用 說明：	
7.1.1.3	是否透過帳號、密碼等識別方式以識別資料交換操作的使用者身份，且若有多名操作人員，是否以個別之帳號、密碼登入？			□ 適用 □ 不適用 說明：	□ 備有有帳號申請紀錄 □ 未有帳號共用情形
7.1.1.4	是否定期(每季或至少半年)檢視物流資料交換操作人員之權限設定，以確認相關開放權限皆為職務所需？			□ 適用 □ 不適用 說明：	□ 備有每季權限審查紀錄
7.1.1.5	電子商務網路平台、店家或供應商之物流資料交換需求，考量提供單次、每日或每月之資料交換報表查詢功能，以確保傳輸資料之完整與正確性？	II		□ 適用 □ 不適用 說明：	□ 提供資料交易查詢功能(包括傳送內容、檔案大小、接收時間與狀態等)
7.1.1.6	與電子商務網路平台、店家或供應商之物流資料交換軌跡是否已記錄，並妥善保存至少一年以上？	II	◎	□ 適用 □ 不適用 說明：	□ 備有資料交換紀錄 □ 保留期限少於一年
7.2 配送資料傳遞過程的儲存媒體保護					
7.2.1 應保護內有客戶資料之實體媒體交換，並採用可靠的傳遞管道。					
7.2.1.1	因業務需求，需利用實體傳遞管道交換內存客戶資料之媒體時，是否先將媒體中之客戶資料予以加密，或將其裝入專用信封並密封後再行交付？			□ 適用 □ 不適用 說明：	
8.建立資安通報管理機制					
8.1 電子商務資安通報機制					
8.1.1 應參照電子商務資安通報機制規範，進行資安事故外部通報。					
8.1.1.1	是否建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常等)與個資外洩危機通報與處理機制？	II	◎	□ 適用 □ 不適用 說明：	
8.1.1.2	員工及外部使用者是否知悉資安及個資外洩事件通報窗口及處理程序？			□ 適用 □ 不適用 說明：	□ 公告資安事件通報程 □ 辦理人員認知訓練

編號	實作查檢項目	類別	進階指引	適用情形	實作紀錄
8.1.1.3	是否建立資訊安全事件通報的聯絡窗口，並能夠依據權責提報管理階層以充分與及時回應？			□ 適用 □ 不適用 說明：	□ 聯絡清單公告地點：_____
8.2 資安事故管理					
8.2.1 應建立資安事件與個資外洩通報程序，並對內外部員工宣導相關通報流程。					
8.2.1.1	是否參考電子商務資安通報機制規範，建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常等)之外部通報與提報程序？	II	◎	□ 適用 □ 不適用 說明：	
8.2.1.2	是否具體落實外部通報作業？			□ 適用 □ 不適用 說明：	
8.2.1.3	是否隨時接收外部重大資安資訊，並立即採取必要反應行動？	II		□ 適用 □ 不適用 說明：	
8.2.2 應收集、保存及呈現資安事故之完整證據，並針對事故之原因進行檢討分析。					
8.2.2.1	是否舉行資安事件後之檢討會議，以協助公司能從資安事件中學習？			□ 適用 □ 不適用 說明：	
8.2.2.2	是否就已發生之資安或個資外洩事件，訂有調查程序，以確認事件原因，並據以修正事故預防及處理機制，防範事故再度發生？	II		□ 適用 □ 不適用 說明：	
8.2.2.3	資安事件中相關證據資料是否有適當保護措施以作為問題分析及法律必要依據？	II	◎	□ 適用 □ 不適用 說明：	
8.2.2.4	資訊安全事件處理的過程是否均留有完整紀錄？如有必要，應經由直接發送的電子郵件或網站首頁即時回報事件予相關產業供應鏈上下游業者與消費者。	II	◎	□ 適用 □ 不適用 說明：	□ 備有資安事件紀錄

資料來源：本計畫整理

陸、附錄

一、參考文件索引表

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
策略目標：1.促進公司資訊安全管理			
1.1 資訊安全框架	1.1.1	ISO 27001 4.2	
		ISO 27001 4.3	
		ISO 27001 A.6.1.1	
		ISO 27001 A.6.1.2	
		ISO 27001 A.6.1.3	
		ISO 27001 A.6.1.8	
	1.1.2	ISO 27001 A.10.10.1	
		ISO 27001 6	
1.2 資訊資產風險管理	1.2.1	ISO 27001 4.2	「電子商務交易安全規範-網路平台」
		ISO 27001 A.7	
		ISO 27001 A.14	
1.3 人力安全管理	1.3.1	ISO 27001 A.8.1.2	
	1.3.2	ISO 27001 A.8.2.1	
		ISO 27001 A.8.2.2	BS 10012 4.3
		ISO 27001 A.8.3.2	
		ISO 27001 A.8.3.3	
		ISO 27001 A.8.2.3	
	1.3.3	ISO 27001 A.8.1.1	
		ISO 27001 A.8.1.3	ISO 27011
1.4 遵循性管理	1.4.1		「電子商務交易安全規範-網路平台」
1.5 客戶及第三方管理	1.5.1	ISO 27001 A.6.2.2	
		ISO 27001 A.6.2.3	
		ISO 27001 A.6.2	
		ISO 27001 A.10.10.1	
		ISO 27001 A.8.3.3	
		ISO 27001 A.6.2.1	
		ISO 27001 A.10.2.2	
		ISO 27001 A.11.2.4	
策略目標：2.加強核心資訊系統安全管理			
2.1 核心資訊系統取得、開發及維護安全管理	2.1.1	ISO 27001 A.12.1	「電子商務交易安全規範-網路平台」
	2.1.2	ISO 27001 A.12.2.1	「電子商務交易安全規範-網路平台」
	2.1.3	ISO 27001 A.12.4.1	
		ISO 27001 A.12.5.2	
		ISO 27001 A.12.4.2	

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
	2.1.4.	ISO 27001 A.12.5.1	
		ISO27001 A.15.1.2	
		ISO 27001 A.12.5.5	
		ISO 27001 A.12.6.1	
2.2 核心資訊系統存取控制管理	2.2.1	ISO 27001 A.11.2.1	
		ISO 27001 A.11.2.2	
		ISO 27001 A.11.4.1 A.11.4.2	
		ISO 27001 A.11.5.2	
		ISO 27001 A.11.2.3	
		ISO 27001 A.11.3.1	
		ISO 27001 A.11.5.1	
		ISO 27001 A.11.5.3	
	2.2.2	ISO 27001 A.10.1.3	
	2.2.3	ISO 27001 A.11.5.4	
		ISO 27001 A.11.5.5	
2.3 核心資訊系統資料庫安全管理	2.3.1	ISO 27001 A.11.4.5	PCI-DSS 1.3.7
		ISO 27001 A.11.4.6	
		ISO 27001 A.11.6.1	PCI-DSS 3.4.1
	2.3.2	ISO 27001 A.10.3.1	
		ISO 27001 A.10.10.2	
		ISO 27001 A.13.2.1	
	2.3.3		「電子商務交易安全規範-網路平台」
		ISO 27001 A.10.10.4	
		ISO 27001 A.10.10.1	
策略目標：3.保護客戶個人資料檔案安全			
3.1 客戶資料隱私管理原則	3.1.1	ISO 27001 A.15.1.4	
	3.1.2		BS 10012 4.1
			BS 10012 4.10
	3.1.3		BS 10012 4.4
3.2 客戶資料依法對外公開、資訊揭露作業	3.2.1		BS 10012 4.15
	3.2.2		BS 10012 4.1
3.3 客戶資料取得、處理、儲存及其機密性與正確性管理	3.3.1	個資法第 19 條	
		個資法第 8 條	
		個資法第 3 條	BS 10012 4.10
	3.3.2		BS 10012 4.1
		ISO 27001 A.8.3.3	BS 10012 4.2
		ISO 27001 A.8.1.3	
		ISO 27001 A.11.5.2	
			BS 10012 4.10

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
			BS 10012 4.12
		個資法第 11, 13 條	BS 10012 4.10
	3.3.4	ISO 27001 A.12.2.1	BS 10012 4.10
3.4 客戶資料使用及傳輸安全作業	3.4.1	ISO 27001 A.10.7.4 A.10.8.3	
		ISO 27001 A.10.8.4	
		ISO 27001 A.10.8.2	
		ISO 27001 A.10.10.2	
		ISO 27001 A.10.7.3	
		ISO 27001 A.11.5.2	
		ISO 27001 A.11.4.6	
3.5 客戶資料刪除及停止利用作業	3.5.1	ISO 27001 A.10.7.2	
	3.5.2	ISO 27001 A.10.7.3	
策略目標：4.加強託運單安全管理			
4.1 託運單資料管理	4.1.1	ISO 27001 A.15.1.4	
		ISO 27001 A.10.5.1	
		ISO 27001 A.10.7.3	
		ISO 27001 A.12.3.1	
4.2 紙本託運單之保存及銷毀管理	4.2.1	ISO 27001 A.11.3.3	
		ISO 27001 A.10.7.3	
		ISO 27001 A.9.1.2	
		ISO 27001 A.9.1.4	
		ISO 27001 A.15.1.3	
	4.2.2	ISO 27001 A.10.7.3	
		ISO 27001 A.10.7.2	
		ISO 27001 A.15.1.3	
4.3 託運單調閱與印製作業管理	4.3.1	ISO 27001 A.10.10.1	
		ISO 27001 A.10.7.3	
		ISO 27001 A.11.4.6	
策略目標：5.加強作業環境安全管理			
5.1 作業與辦公環境安全管理	5.1.1	ISO 27001 A.9.1.1	
		ISO 27001 A.9.1.5	
		ISO 27001 A.8.3.2	
		ISO 27001 A.9.2.1	
		ISO 27001 A.10.7.1	
		ISO 27001 A.10.10.1	
		ISO 27001 A.9.1.4	
		ISO 27001 A.8.3.2 A.9.1.2	
		ISO 27001 A.13.1.1	
	5.1.2	ISO 27001 A.10.10.1	
		ISO 27001 A.9.2.5	

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
5.2 營業用電腦設備環境與設備安全管理	5.2.1	ISO 27001 A.9.1.2	
		ISO 27001 A.9.2.3	
		ISO 27001 A.9.2.2	
		ISO 27001 A.9.2.1	
		ISO 27001 A.9.2.4	
			「電子商務交易安全規範-網路平台」
	5.2.2	ISO 27001 A.9.2.7	
		ISO 27001 A.10.7.3	
		ISO 27001 A.10.5.1	
		ISO 27001 A.9.2.6	
策略目標：6.加強網路安全管理			
6.1 網路通訊與資訊作業安全管理	6.1.1	ISO 27001 A.10.4.1	
	6.1.2	ISO 27001 A.10.5.1	
	6.1.3	ISO 27001 A.10.6.1	OWASP 4.4 (OWASP-AT-001-010)
		ISO 27001 A.10.3.1	ISO 27011
		ISO 27001 A.6.2.3	ISO 27011
			「電子商務交易安全規範-網路平台」
	6.1.4	ISO 27001 A.10.6	
		ISO 27001 A.11.4.4	
		ISO 27001 A.11.4.5	
		ISO 27001 A.11.5.2 A.11.6.1	
	6.1.5	ISO 27001 A.10.10.1	
		ISO 27001 A.10.10.3	
		ISO 27001 A.10.10.2	
		ISO 27001 A.10.10.4	
	6.1.6	ISO 27001 A.10.10.6	PCIDSS 10.4
	6.1.7	ISO 27001 A12.6.1	
6.2 電子郵件安全管理	6.2.1	ISO 27001 A.11.2.1	
		ISO 27001 A.10.6.1	
		ISO 27001 A.15.1.3	
	6.2.3	ISO 27001 A.11.4.6	
6.3 個人資訊設備安全管理	6.3.1	ISO 27001 A.12.4.1	
	6.3.2	ISO 27001 A.11.3.1	
		ISO 27001 A.10.1.2	
		ISO 27001 A.10.7.1	
		ISO 27001 A.11.3.3	
		ISO 27001 A.15.1.5	
策略目標：7.建立外部單位資料交換安全管理			
7.1 配送資料交換	7.1.1	ISO 27001 A.12.3.1	

管理項目	要求項目	依據之法規或標準	其他可供規範實作之參考
協議與保護措施		ISO 27001 A.10.8.1	
7.2 配送資料傳遞過程的儲存媒體保護	7.2.1	ISO 27001 A.10.8.3	
策略目標：8.建立資安通報管理機制			
8.1 電子商務資安通報機制	8.1.1	ISO 27001 A.13.1	
8.2 資安事故管理	8.2.1	ISO 27001 A.13.1	「電子商務資安通報機制規範與作業要點」
	8.2.2	ISO 27001 A.13.2	

二、規範常見名詞釋義

項次	名詞	定義說明	備註
1	風險評鑑	風險分析與風險評估的整個過程。	
2	風險	威脅利用弱點對資訊資產所造成影響之可能性。	
3	風險評估	把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。	
4	風險分析	系統性的使用資訊，以識別緣由與估計風險。	
5	威脅	危及資訊資產的外在因素，如天然災害、惡意攻擊等。	
6	脆弱點	指資訊資產內部可能遭受威脅利用之處。	
7	螢幕淨空	當設備無人看管或使用時宜將個人電腦和終端機保持在登出或鎖定狀態，以通行碼等授權機制保護的螢幕及鍵盤上鎖機制保護。	
8	惡意程式、惡意碼	故意建立用來執行未經授權並通常是有害行為的軟體程序，包括病毒、後門程序、鍵盤紀錄器、密碼盜取者和其它木馬程序、Word 和 Excel 病毒、木馬、犯罪軟體、間諜軟體和廣告軟體。	
9	行動碼	由遠端系統透過網路轉存入本機端進行代理作業，可進行下載或在本機端上執行沒有明確安裝或者接受者的作業。包括 include scripts(Java 腳本，VBScript)、Java 小應用程式，ActiveX 控制，flash 動畫。	
10	安全容量	系統或網路的資源使用宜監控、調校、及預估未來容量需求，以確保服務可有效運作。	
11	時間同步	業務營運相關系統宜與議定的準確時間(如中原	

項次	名詞	定義說明	備註
		標準時間、NTP 或其他公正單位)進行時間校正與同步作業。	
12	委外廠商	第三方委外單位、第三方合作業者，含物流商、供應商及服務商等。	
13	利害相關團體	執法機關、政府緊急應變中心、客戶、產業供應鏈上下游業者、電子商務資安事件通報機制。	
14	儲存媒體	資料儲存媒介，例如：紙本文件、電腦媒體(磁片、磁帶、記憶卡、外接硬碟與光碟片)。	
15	可攜式設備	包括筆記型電腦、PDA 等。	
16	密碼、加密	Cryptographic，將正常的(可識別的)資訊轉變為無法識別的信息。	
17	通行碼	Password，對應帳號的登入密碼，使用者在存取資訊系統與服務前，依使用者授權用來查證其身份的方法。	
18	資訊安全事件	information security event 系統、服務或網路狀態經鑑別而顯示示可能有違反資訊安全政策或保護措施失效，或可能與安全有關但事先未知狀況的發生。	
19	TWCA	臺灣網路認證公司，提供國內網路安全認證服務，為國內最大的民間憑證發行機構。	
20	PCIDSS	Payment Card Industry Data Security Standard，支付卡產業相關標準指引與要點，由 Visa International、MasterCard Worldwide、 American Express、Discover Financial Services 及 JCB 等支付卡產業安全標準委員會提出，目的在幫助公司保護支付卡帳戶資料。	1.2.1 版，2009 年 7 月版
21	保密協議	透過保密切結書、合約書等文件規範相關保密要求。	參照 ISO 27002-6.1.5
22	社交工程	利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。	
23	即時通訊軟體	如 msn、yahoo 即時通、Google Talk、Skype 等軟體，可使用網路即時的傳遞文字訊息、檔案、語音與視訊交流。	