欣欣大眾市場股份有限公司資訊安全管理辦法

壹、依據

「金管會金融機構資通安全防護基準」、「行政院及所屬各機關資訊安全管理要點」及「資訊安全管理規範」、「資通安全管理法施行細則」、「欣欣大眾市場股份有限公司 2024 年永續報告書」。

貳、目的

為有效確保公司各類資訊系統安全，杜絕人為因素可能造成對公司資訊系統之危害及損失。

參、執行方式

一、設置資訊室專業單位，執行公司內部及外部網路漏洞偵測網路漏洞、杜絕資料外洩，防範資訊資產遭外部蓄意入侵或內部不當使用、洩漏、竄改、破壞等情事

二、**「資訊室」職掌**

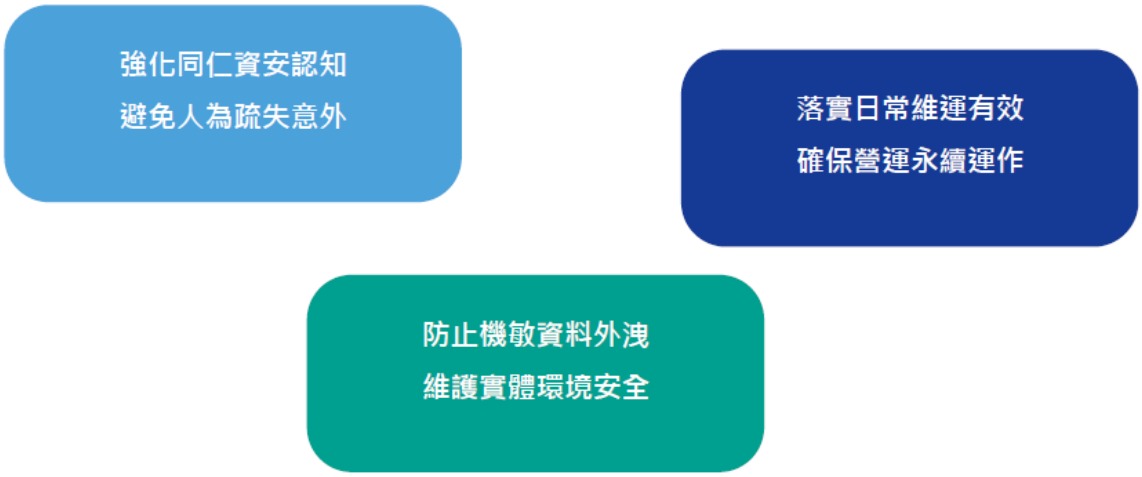
1、負責公司資訊安全制度之規劃、監控及執行資訊安全管理作業資訊安全計畫擬定。

2、資訊安全事件檢討及改善。

三、稽核單位每年依照稽核計畫安排資訊循環相關查核，評估公司資訊作業內部控制之有效性。

資通安全政策示意圖

資通安全政策



肆、內部管控作業示意圖

不定期辦理資訊安全及個人資料保護教育訓練及宣導作業，新進人員皆須簽訂保密協定。

聘用／委任可能接觸機密性或敏感性資訊之人員，應有適當安全評估；人員職務調動或離職時，相應存取權限應即時調整。

定期評估並更新資訊安全政策，以確保其符合相關法令規範；定期執行安全評估，確保若有資通安全事件發生，可即時並適當的回應與處理。

個人電腦均安裝防毒軟體且定期更新病毒碼，禁止使用未經授權的軟體；使用者登入帳號及密碼有專人管理，並要求同仁定期更換系統密碼維護帳號安全；外部連線應有防火牆等安全。

重要資訊系統或設備已建置適當備份或監控機制，定期進行復原及應急防範演練。

人員管理－保密防火牆作業	• 本公司董事、獨立董事、經理人及受僱人應以善良管理人之注意及忠實義務，本誠實信用原則執行業務並簽署保密協定。 • 知悉本公司內部重大資訊之董事、獨立董事、經理人及受僱人不得洩露所知悉之內部重大資訊予他人。 • 本公司之董事、獨立董事、經理人及受僱人不得向知悉本公司內部重大資訊之人探詢或蒐集與個人職務不相關之公司未公開內部重大資訊，對於非因執行業務得知本公司未公開之內部重大資訊亦不得向其他人洩露。
物－保密防火牆作業	• 內部重大資訊檔案文件以書面傳遞時，應有適當之保護。 • 以電子郵件或其他電子方式傳送時，須以適當的加密或電子簽章等安全技術處理。 • 公司內部重大資訊之檔案文件，應備份並保存於安全之處所。
運作管理－保密防火牆作業	本公司應確保前二條所訂防火牆之建立並採取下列措施： 一、採行適當防火牆管控措施並定期測試。 二、加強公司未公開之內部重大資訊檔案文件之保管、保密措施。

伍、資訊安全列為公司管理重大主題

重大主題	對應 GRI 對應 SDGI	對欣欣百貨意義	價值鏈衝擊邊界 涉入程度：●直接／○間接（促成或商業關係） 衝擊評估：▲正面衝擊；□負面衝擊					管理措施揭露章節（補救負面衝擊的）
			政府單位 主管機關	股東 投資人	供應商 承包商	客戶	員工	
資訊安全與客戶隱私	GRI 418: 客戶隱私	面對《個資法》須強化資安防護與制度管理，避免罰鍰與法律責任。透過資訊安全與隱私保護，符合法規要求，提升品牌形象。	○	○	●	●	●	2.6 資訊安全
			□	□	▲	▲	▲	

陸、公司治理重大主題揭露項目

GRI 準則	揭露項目	章節	頁碼	省略 / 備註
重大性主題：資訊安全與客戶隱私				
GRI 3: 重大主題揭露	3-3 重大主題管理	2. 公司治理	33	
GRI 418: 客戶隱私	418-1 客戶個人資料外洩的申訴案件	2.6 資訊安全	44	

柒、SASB 準則揭露索引表

指標代碼	會計指標	指標單位	對應章節	頁碼
揭露主題：零售及物流服務的能源管理				
CG-MR-130a.1	(1) 總能源耗損 (2) 能源採用外購電力占總耗電百分比 (3) 採用再生能源的比例	千兆焦耳、百分比 (%)	4.3 節能減碳	59
揭露主題：數據安全				
CG-MR-230a.1	說明鑑別及因應資料安全風險的方法	n/a	2.6 資訊安全	42
CG-MR-230a.2	(1) 資料外洩次數	件數	2.6 資訊安全	42
	(2) 涉及個人識別資訊 (PII) 外洩之比例	百分比 (%)	2.6 資訊安全	42
	(3) 帳戶持有人受影響個數	件數、百分比 (%)	2.6 資訊安全	42

捌、資訊安全強化作為

持續更新電腦病毒碼以防範資訊安全威脅	為防堵駭客入侵及電腦病毒攻擊，公司持續執行公務電腦病毒碼的定期更新工作，確保所有設備維持在最新防護狀態，降低潛在資安風險。
委外專業廠商維運資訊系統並強化資安	持續委外專業部門執行以下各項系統之軟硬體維護及資安確保作業： • 銷售時點情報系統 (Point of Sale,POS) • 電子郵件服務 • 內部資訊網路 • 公司官方網站 藉由專業技術資源投入，提升資訊系統穩定性與資安防護水準。
強化 POS 系統機房實體隔離措施	已完成「POS 系統機房」的實體隔離強化作業，透過實體環境區隔與安全機制設置，有效提升機房整體安全性，防止未經授權進入及潛在資安事件發生。
建立公務資料雲端備援機制	為保障公司公務資料之安全與持續可用性，已完成建立「雲端存儲」備援機制，可於發生設備故障或災害時即時還原資料，確保資料完整與營運不中斷。
監督委外廠商資訊保管責任落實	針對公司各類委外執行項目（如系統維護、保全、機電、清潔等），持續落實監督廠商對其所知悉公司資訊之保密、保管與合法使用義務，確保資訊不外洩或被濫用。
資訊系統使用者權限管理與稽核作業	公司持續落實內部資訊安全管控機制，包括： • 定期及不定期內部稽核 • 使用人員（如 POS、公務郵件等系統）權限審查與管理以確保公司整體資訊安全及會員個資之保護。 • 2024 年無個資外洩事件。

玖、資訊安全與客戶隱私

對應主題	資訊安全與客戶隱私風險管理	
GRI 指標	GRI 418: 客戶隱私	
政策與承諾	我們致力於建立資通安全的企業文化，為建立本公司良好之內部重大資訊處理及揭露機制避免資訊不當洩漏，並確保本公司對外界發表資訊一致性與正確性，資安措施不斷進步，與時俱進。	
衝擊	**正面衝擊**	**負面衝擊**
	妥善保護公司與其商業夥伴（如專櫃廠商）個人資料（員工與消費者），維護利害相關者權益。	產生資安漏洞或遭受駭客網路攻擊，導致客戶個資或企業機敏資訊外洩，營運中斷，侵害客戶等利害關係人權益。
行動方案	**預防與減緩**	欣欣百貨設有資安長，全面性就技術、程序、營運、法令遵循、風險控管等不同層面，強化企業資訊安全並建立資安預警與通報機制，降低企業資安風險。
	行動措施	關於員工與顧客個資保護，欣欣百貨檢視個資使用及保存情況，以確保個資被適當保護及管理，以符合《個人資料保護法》規範。
利害關係人議合	為保障客戶個人資料安全與隱私，訂有「客戶資料保密措施」，設立資訊安全組織，負責處理有關資訊安全預防及危機處理最短時間內恢復正常運作，降低事故可能帶來之損害。	
評估與追蹤	·由資安長負責統籌並執行資訊安全政策，宣導資訊安全訊息，提升同仁資安意識，不定期進行資訊安全檢查，強化資訊安全管理。 ·稽核單位每年依照稽核計畫安排資訊循環相關查核，評估公司資訊作業內部控制之有效性。	

拾、其他資訊安全要求

1、公務用個人電腦(筆電)均須安裝防毒軟體、設置使用人帳號及密碼，並每六個月更換乙次。

2、各類資訊系統均須安裝防毒軟體、設置管理者權限及帳號、密碼，並每六個月更換乙次。

3、嚴禁將公司公務攜回家辦。

4、嚴禁使用個人存儲裝置執行公司資料交換或下載。

5、資訊系統伺服器均須安裝防火牆防護。

6、系統須具備資料自動備份功能。

7、系統須具備異常時自動示警功能。

8、系統須具備稽核「使用者紀錄」、「登入及登出系統之日期及時間」、「登入位址 IP」功能。

9、防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。

10、系統維護合約商，未經公司同意，不得擅自執行系統調校。

11、定期演練備援作業程序，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

12、廠商提供之資訊媒體，於使用前須執行掃毒，確保無感染電腦病毒。

13、要求公司全體人員重要公務資料每週五下班前上傳公司異地備援伺服器，確保重要公務資料不因系統或裝備故障造成資料散失。

14、持續落實要求公司人員恪遵 WiFi 使用規定，確保公司網路與外部確實有效隔離，完善公司資訊安全環境。

15、電腦設備如遭病毒感染，應立即離線(拔除網路線連結)，並執行病毒清理完成後，方可重新連線；資安事件通報圖(如附圖)。

16、資訊系統之運作功能及資料存取應依據「個人資

料保護作業要點」相關規定辦理。

17、同仁應遵守公司資訊安全政策之相關規定，違者按情節輕重依「公司工作規則」相關規定議處。

18、同仁應遵守業務機密之相關法令規定，在職及離退職後均不得洩漏所知悉之資訊機密，或為不當之使用，違者追究法律責任。

19、資訊室應配合稽核室定期執行公司資訊安全稽核作業。

拾壹、本管理辦法視實際運作，適時修訂或補充之。

欣欣大眾市場股份有限公司資通安全風險管理架構圖