資通安全管理

1.資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等

(1)資通安全風險管理架構

A.本公司由資訊部負責資訊安全政策管理與規劃，以及資訊安全相關事件處理與通報。

B.資訊部為非隸屬使用者單位之獨立部門，負責統籌並執行資訊安全政策，宣導資訊安全訊息，提升員工資安意識，蒐集及改進組織資訊安全管理系統績效及有效性之技術、產品或程序等。

(2)資通安全政策

在個人資料保護及資訊安全的內控制度上，本公司訂有「個人資料保護之管理」、「資訊循環」及「資訊安全管理辦法」，對系統權限、設備安全、個人資料維護、資安事件等進行規範。在資安核心目標上，因本公司專注於服務零售客戶，而對於零售業而言，最常見的資安問題為「消費詐騙」:即竊取會員資料及訂單資料進行詐騙等。本公司現階段資安保護核心的「消費者個人資料」為包括：會員資料、訂單與信用卡資訊。針對信用卡資訊的處理，在儲存、傳輸、處理消費者付款信用卡認證之訊息皆有加密機制。基於縱深防禦之上，本公司採「滾動式持續優化」策略，從事前管理、事中應變及事後優化三大面向改善資安。在事前管理部分，包括即時監控，偵測與辨識資安攻擊；事中應變部分，則是在資安事件發生時，能快速回應，進行資安保護以控制事件；事後優化部分，在資安事件發生後，記取教訓，經由事後優化持續改善資安作為，改善本公司資安體質。本公司特別重視消費者個資安全的保護，針對常態需取得消費者個資（如：客服單位等）的電腦設備採更嚴謹的管制措施，具體說明如下：

A.增強的趨勢端點防護

針對客服單位，本公司啟用增強型的偵測模組：行為監控模組、機器學習防護模組、周邊媒體控管模組、軟體白名單控管模組等。上述模組皆能有效提升電腦的異常行為的偵測能力，並能在威脅發生時，及時通知資安人員進行事件處理。

B.數據分析軟體

資安專責單位，同時收攏所有系統的稽核日誌，並將相關日誌進行數據分析，針對特定的關係客體（客服人員等）、以及相關行為（地、物、時間、資料量）等進行關聯性的分析，來發掘潛在的資安威脅，以利資安人員能夠快速掌握狀況，並提高辦公室電腦的使用安全。

(3)具體管理方案

A.辦公室網路安全

本公司在辦公室對外的網路端口節點，已佈署中華電信-資安艦隊之防火牆，此防火牆在資訊流量往返公司內網與網際網路間，其內建的威脅模組會即時進行威脅的控管與追蹤，針對異常流量發出告警，告知資安人員即時處理。本公司同時在辦公區電腦佈署端點防護措施，其特點為機器學習與特徵分析，如果惡意程式夾藏在檔案與加密流量中，且惡意程式到達端點時，端點防護措施會比對相關的特徵碼及程式行為，對威脅進行隔離，以達保護辦公室設備使用安全之目的。

B.防範惡意網路攻擊

本公司為整體系統運作效能最佳化，採用網路負載平衡（Load-Balancing）機制，由兩台以上虛擬主機一起提供相同服務。

C.應用層防禦

本公司透過網站防火牆，保護網頁應用程式及伺服器，以阻擋同一 IP 來源的大量惡意流量，或常見的 SQL Injection 資料庫語法攻擊等。

D.基礎設施層防禦

本公司使用中華電信 Hi-Link VPN 及資安艦隊等防火牆功能，在攻擊可即時自動監控系統狀況，同時隔離攻擊目標並即時提供團隊應調整系統配置、阻擋攻擊規則、隔絕受攻擊主機。

E.日常維運改善與演練

本公司定期進行內部對焦與測試，調整防禦相關設定，提升防禦強度。

F.針對消費者個人資料保護

本公司已協助客戶，依個資保護法第 6 條，提供隱私權聲明條款(會依相關法令及事項更新)，告知消費者有關個資蒐集、處理或利用之相關事項。在消費者申請會員購物時，消費者須同意本公司官網或客戶的隱私權聲明才能申請會員進行消費，且消費者個資資料係客戶所有，相關安全儲存加密已規範於資安相關措施中。

G.重要資料之控管權限及機密資料之保管措施

本公司內部對於重要資料之控管權限及機密資料之保管措施以防範個資外流已進行系統權限管理，對各部門、各職級所能存取之系統或權限有明確分級，並每年重新檢視權限之設定有無調整需要。而在機密資料之傳輸與儲存上，本公司資料傳輸採用安全加密，可防止資料透過網路傳輸時，被惡意攔截、監聽或修改等。也可保護被不當取得之資料仍具有保密性，無法被讀取。

(4)投入資通安全管理之資源

本公司組織運作係以團隊為主，目前與資安相關之團隊共計 3 名，含資安專職人員共 1 名，年度資安預算編列依防護需求持續投入。

2.列明最近二年度及截至公開說明書刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者應說明其無法合理估計之事實：無。