資通安全管理之資訊揭露

一、資通安全管理策略與架構：

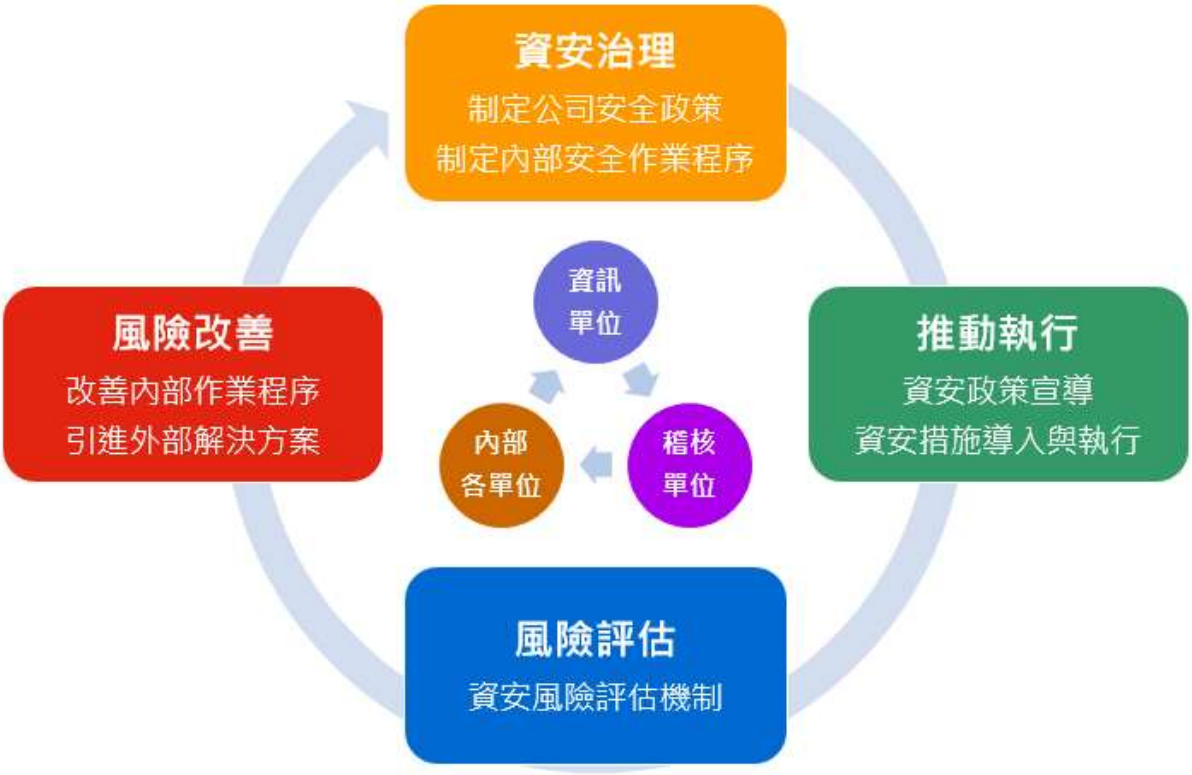
(一)資通安全風險管理架構

1. 企業資訊安全治理

三商家購公司為維護公司競爭優勢與寶貴的智慧財產，於民國 112 年成立「資訊安全管理專屬單位」，並配置資安專責主管 1 名及 1 名資安專責人員與 2 名資安承辦人員，合計 4 名，主係確保資通安全管理制度之運作，並訂定資訊安全管理政策，以強化本公司資訊安全管理，確保資料、系統、設備及網路安全，保障公司與全體員工之權益，並全面提升資安意識。為確保相關資訊系統的運作風險得以有效控制，「資訊安全管理專屬單位」每年至少召開一次檢討資安作業，必要時得召開臨時會議，並每年彙總後分別向審計委員會及董事會報告。

2. 資訊安全管理架構

- 本公司資訊安全之權責單位為資訊單位，負責規劃、執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊系統控制存取等管理及推動資訊安全意識。
- 本公司稽核單位為資訊安全監理之查核單位，若查核發現缺失，即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低資安風險。
- 組織運作模式採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



(二)資通安全政策

1. 資通安全之目標：
為貫徹本公司各項資訊管理制度能有效運作執行，建立安全及可信賴之電腦化作業環境，確保資訊系統、設備網路之安全維運，以保障公司利益及各單位資訊系統之永續運作，達到永續經營目的。

2. 資通安全之範圍：
2.1 人員管理及資訊安全教育訓練。
2.2 電腦系統安全管理。
2.3 網路安全管理。
2.4 系統存取管制。
2.5 系統及維護安全管理。
2.6 資訊資產安全管理。
2.7 實體及環境安全管理。
2.8 資訊安全稽核。

3. 資訊安全的原則及標準：

3.1 不定期資訊安全宣導，包括資訊安全政策、資訊安全法令規定、資訊安全作業程序、資訊安全案例以及如何正確使用資訊科技相關設施等，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工對資訊安全意識，並遵守資訊安全規定。

3.2 為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。

3.3 為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

4. 資訊安全具體管理措施

項目	具體管理措施
權限管理	人員帳號、權限管理與系統操作行為之管理措施： ● 人員帳號權限管理與審核。 ● 人員帳號權限定期盤點。
存取管控	人員存取內外部系統及資料傳輸管道之控制措施： ● 內部網路、DMZ 網段、測試網段與外部網路之連線存取均需透過防火牆之安全進行管控。 ● 使用自動網站防護系統控管使用者上網行為。 ● 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
外部威脅	潛在弱點、中毒管道與防護措施： ● 使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。 ● 使用軟體及作業系統定期更新。 ● 有自動郵件掃描威脅防護，如不安全的附件檔案、釣魚郵件、垃圾郵件，及惡意連結。
系統可用性	系統可用狀態與服務中斷時之處置措施： ● 重要資訊系統定期由專業顧問檢查、調整及優化。 ● 各部門重要檔案存放於伺服器，由資訊單位統一備份保存。 ● 重要資訊系統資料庫皆設定每日備份 ● 定期進行災害復原演練。

網路、系統安全	● 委託專業的資安專家不定期執行公司內部資安健診；檢視內部網路架構及惡意活動檢視、使用者電腦及伺服器主機惡意活動檢視改善，提高企業內部網路及系統安全。
應用程式安全	● 對外服務平台委託專業資安廠商進行網站弱點掃描、滲透測試檢測。 ● 導入 Web 應用程式防火牆(WAF)持續強化應用程式安全控管機制。
教育訓練與宣導	● 加強員工對郵件攻擊的警覺性，不定期執行社交工程演練，提升員工資安意識。
情資蒐集	● 加入「台灣 CERT/CSIRT 資安聯盟」，進行資安情資交流。

5.資通安全的資源投入

針對系統主機的作業系統或重要軟體升級、災害復原演練、系統備援等重要的資安工作，資訊單位定期檢討規劃與執行進度，並透過不定期的社交工程演練、資安健檢服務等，判斷使用者的資訊安全觀念是否足夠、資訊設備資源投入與系統配置是否存在漏洞，編列資安預算後執行。

6.緊急通報程序

當發生資訊安全事件時，發生單位通報資訊責單位，判斷事件類型並找出問題點，立即處理並留下紀錄。

7.112 年度投入資通安全管理之資源及執行成果

7.1 強化資通安全架構

- 4 月委託外部資安專業公司針對 Go 美廉電子商務平台進行網站弱點掃描及滲透測試，以強化網站安全。
- 9 月委託外部資安專業公司針對美廉 APP 進行行動應用 App 基本資安檢測並取得「行動應用 App 基本資安標章」。
- 10 月網站啟用中華電信網站應用防火牆（WAF），以強化網站安全。
- 11 月加入「台灣 CERT/CSIRT 資安聯盟」，進行資安情資交流。
- 本年度已辦理 6 次抽樣備份進行還原演練，確保備份資料還原之可用性。

7.2 員工教育訓練

- 5 月對資訊人員進行外部資安管理訓練課程，共 16 小時。

- 本年度辦理資訊安全教育課程及宣導，共 4 場次，149 人受訓。
- 不定期選取資安事件案例，對全公司進行資訊安全重要性宣導。

7.3 進行社交工程演練

- 對內部員工進行電子郵件社交工程演練之郵件開啟率、點選連結率及附件點閱率，透過演練提升員工郵件使用資安意識。