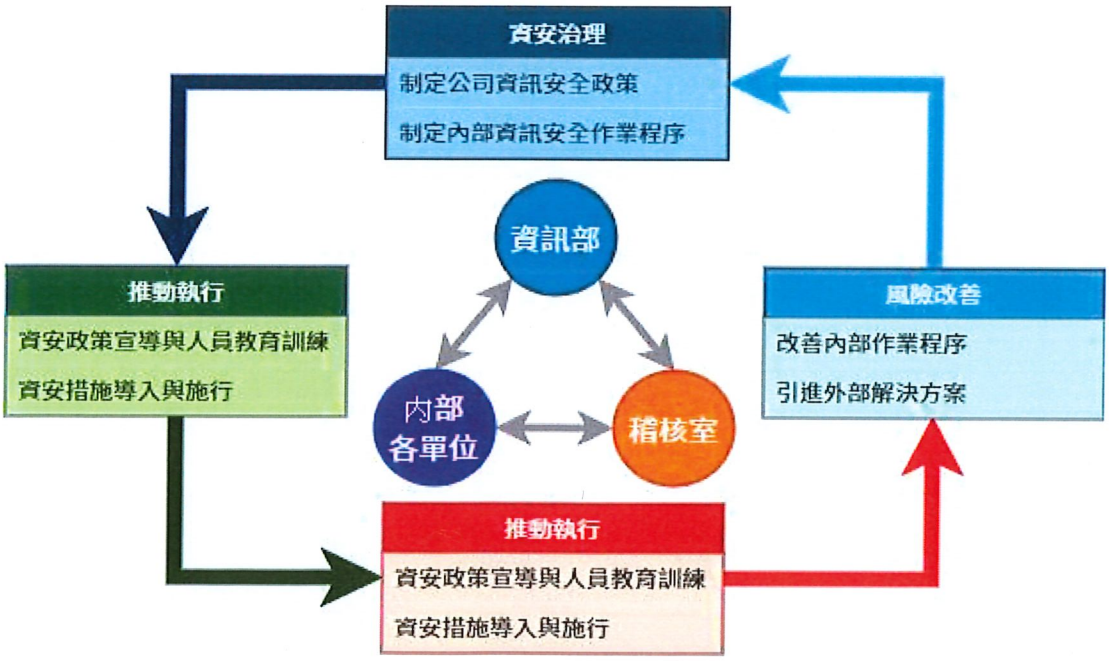
資訊安全政策及管理方案

資訊安全管理

資訊安全風險管理架構

- 本公司資訊安全之權責單位為資訊部，該部設置資安長、資訊主管，與專業資訊人員數名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，並定期報告公司資安治理概況。
- 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，與專職稽核人員數名，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
- 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。



資訊安全政策及具體管理方案

本公司資訊安全管理機制，包含以下三個面向：

（一）制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

（二）科技運用：建置資訊安全管理設備，落實資安管理措施。

（三）人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識。

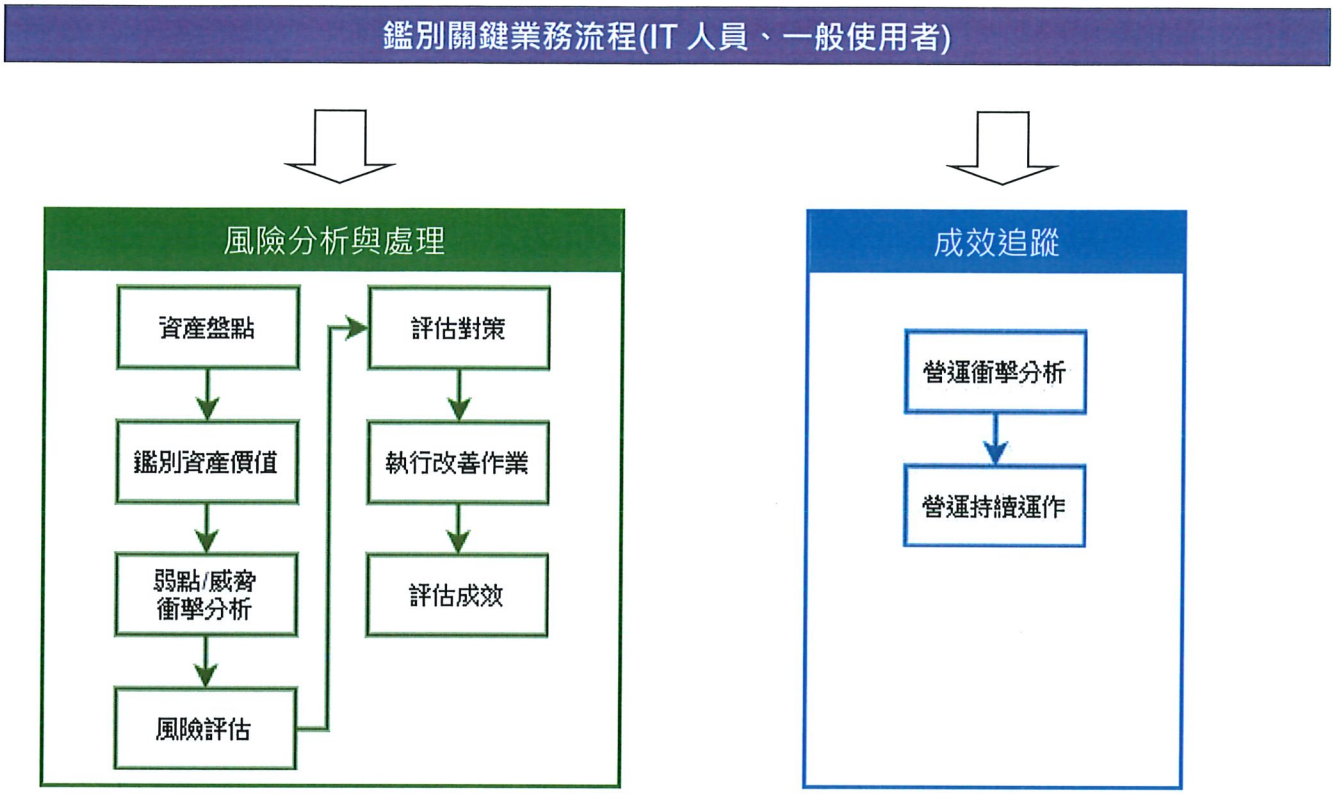
管理措施說明如下：

- 制度規範：本公司內部訂定多項資安規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。
- 科技運用：本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦設計作業程序和導入資安系統工具，落實人員資訊安全管理措施。
- 人員訓練：本公司每季定期實施新進人員資訊安全教育訓練實務課程，並建置數堂線上學習 (E-Learining) 資訊安全課程，藉以提昇內部人員資安知識與專業技能。

資訊安全管理措施

本公司定期審視內部資訊安全規範並報告資安治理概況。

本公司資訊風險評估程序如下：

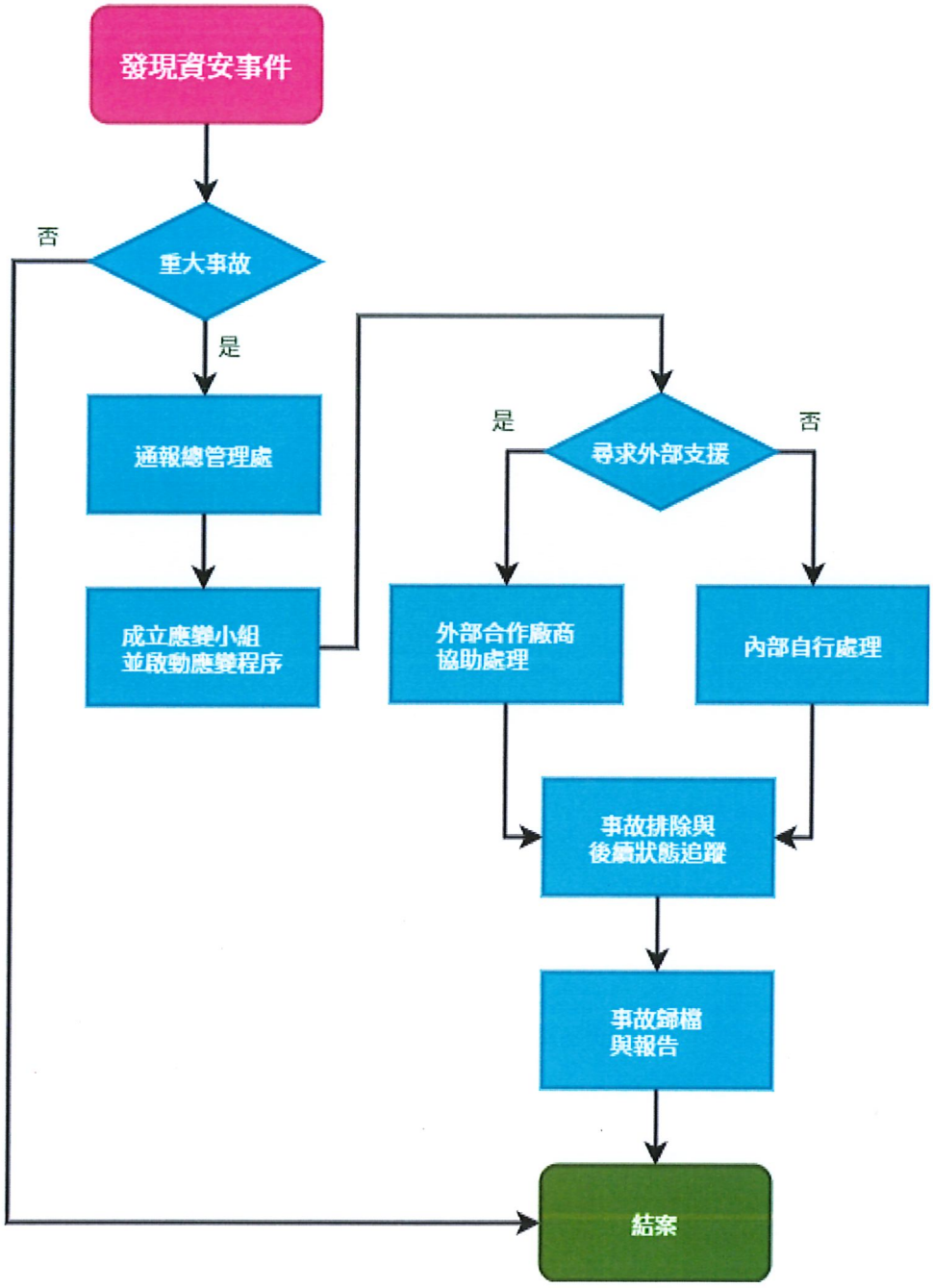


本公司實施之資訊安全管理措施，包含如下：

資訊安全管理措施		
類型	說明	相關作業
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/外部存取管控措施 資料外洩管道之控制措施 操作行為軌跡記錄分析
外部威脅	內部系統潛在弱點、中毒管道、與防護措施	主機/電腦弱點檢測及更新措施 病毒防護與惡意程式偵測
系統可用性	系統可用狀態,與服務中斷時之處置措施	系統/網路可用狀態監控及通報機制 服務中斷之應變措施 資料備份備援措施、本/異地備援機制 定期災害還原演練

資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。



2.5 資訊安全管理

三商投控為確保消費者的個資被完善的保護，除了將「個資風險管理」整合於企業整體風險管理及稽核機制中，定期執行個資盤點、風險分析、制度內評、通報修訂、資料銷毀、教育訓練等工作，也要求總部和門市端同仁們皆需完成個資線上必修課程。

本公司訂有內部個資保護管理通報，對外則於合約加註個資保護條款，確保所有營運單位、供應商及顧客均受到個資保護，同時，我們也利用內評計畫及外部驗證制度，協助各部門持續檢討資訊安全保護系統之有效性，並存有紀錄。針對人員違反公司個資保護管理規則，亦訂定相當的懲處辦法。

• 三商行

三商行為確保會員權益，2024 年進行鞋全家福網站、網頁、APP 等資訊安全檢測。每年也投入適當資源進行 APP 優化升級。以確保會員在使用全家福的網際網路購物以及 APP 使用操作能更加安全，與更優質的購物體驗。

2024 年進行資訊安全檢測包括，網站、網頁、APP 弱點掃描以及滲透測試，以及時發現問題，立即安排時間解決，並規劃 AWS 系統建置之雲端網路環境建置，用心維護會員資料的安全。在 APP 資訊安全提升方面：會員密碼加密包含資料庫加密，忘記密碼作業流程調整，過去以發送密碼簡訊，調整後以發送驗證碼簡訊，後會員可依照收到驗證碼，去重新設定密碼後，再行登入會員，提升會員資料在傳輸過程中的安全性。

【Google 帳戶驗證】為強化 Google Play 平台之資訊透明度，並提升使用者對本公司之信任。全家福於 2024 年 10 月依計畫遵循新版 Google Play 管理中心政策規範完成相關驗證程序，以確保平台營運之合規性與使用者之信賴。

※ 註 1：2023 年 4 月公佈之「Google Play 應用程式帳戶刪除規定」：（1）提供應用程式內路徑，讓使用者刪除應用程式帳戶和相關資料；（2）提供網路連結資源，讓使用者可要求刪除應用程式帳戶和相關資料。

• 三商餐飲

三商餐飲內部則訂有資訊安全管理辦法，內容包含資訊安全事件通報與處理規範。0800 客服在接獲客訴時，會直接予以回覆或交由門市處理，僅會記錄此次客訴內容，不會留存顧客相關個人資訊，留存於錄音主機之來電紀錄也由專人保管及列入個資盤點；三商 i 美食卡 APP 於會員申辦帳號時，必填個資僅有手機號碼及出生西元年月，且須經會員勾選同意服務條款及隱私權政策後方可完成註冊。

為確保完善保護會員個資，資料皆保存於公司系統中並由專人管理，無紙本資料留存，若有相關行銷活動、抽獎活動等需公告名單時亦會將個資進行去識別化，保管期限屆滿或特定目的消失，將依「個資銷毀流程」進行個資銷毀處理。

三商 i 美食卡 APP 與線上訂購平台正式導入 ISO 27001 管理制度，全面強化資訊安全保障，確保會員資料與平台交易過程的安全性與隱私性並且進行進行漏洞掃描與風險評估。通過採用此國際標準，三商餐飲股份有限公司不僅有效降低了資訊安全風險，還顯著提升內部流程管理的效率，並確保各項作業符合法規要求。此外，該制度的實施進一步強化會員對於服務與信任，為未來的永續發展打下良好基礎。

• 三商家購

三商家購遵循「個人資料保護法」建立個人資料保護管理作業程序，2023 年成立了個人資料管理專責單位，負責推動個人資料保護管理事宜，包含定期執行個資盤點、風險分析、制度內評、通報修訂、資料銷毀、教育訓練等工作，並配合人資課程要求總部和門市同仁皆需完成個資線上必修課、定期執行資訊安全 / 社交等演練。

三商家購也於同年成立「資訊安全管理委員會」，設有專責人員，確保資通安全管理制度之運作，並訂定資訊安全管理政策，強化本公司資訊安全管理，確保資料、系統、設備及網路安全，並全面提升資安意識。「資訊安全管理委員會」每年至少召開一次檢討會議，必要時得召開臨時會議，並每年彙總後向董事會報告。範疇包含網路防護、軟硬體防護、資通環境定期檢測、行動 APP 檢測、電子郵件社交工程演練等，並透過內外部資安管理訓練課程、辦理資訊安全教育課程及宣導。2024 年共計 2 次董事會報告，議題範疇包含外部資訊稽核項目改善、門市與 IDC 機房備援網路、資安健診、系統災害復原演練、物流中心無線網路設備更新以及 Go 美廉網站與 APP 資安檢測等。

三商家購每年度執行個資資料盤點作業，並適時修訂「個人資料檔案維護計畫」，加強各單位個資維護意識，並落實各項安全維護措施，以確保本公司各項業務所蒐集、處理及利用之個資能有效進行管理與保護。

資通安全執行情形報告

報告單位：資安室

報告期間：2024年度

報告對象：董事會

114年8月14日

一、資通安全政策概況

- 政策遵循情形：
  已完成內控制度資訊系統控制作業改版。

二、資通安全執行成果

- 加入資安情資分享TWCERT。
- 完成年度資訊資產盤點。
- 資訊安全暨個資安全教育訓練：共辦理1場，125人參與，全部通過測驗。
- 電子郵件社交工程演練：共18人次開啟社交工程郵件，於測試後針對開啟釣魚測試信之同仁進行資訊安全教育訓練。
- 弱點掃描與修補：發現 2 項高風險，已全部完成修補。
- 滲透測試：發現 8 項高風險，已全部完成修補。
- 導入ThreatSonar Anti-Ransomware 威脅鑑識分析與回應平台，防範勒索軟體。
- 導入資通安全威脅偵測管理機制(SOC)。

三、資安事件通報與處理

- 無發生資安事件

四、資安風險與持續改善措施

- 風險辨識：
- 會計師內控制度資訊循環查核，發現員工離職後帳號關閉時效性不一。
- 改善計畫：
- 各部門離職作業流程需更暢通。
- 定期執行帳號盤點。

五、結論與建議

- 本年度運作穩定，無重大資安事件。
- 已規劃具體改善措施，建議持續投入資源強化資安。