資通安全管理：

1.資通安全風險管理架構

(1)企業資訊安全治理組織

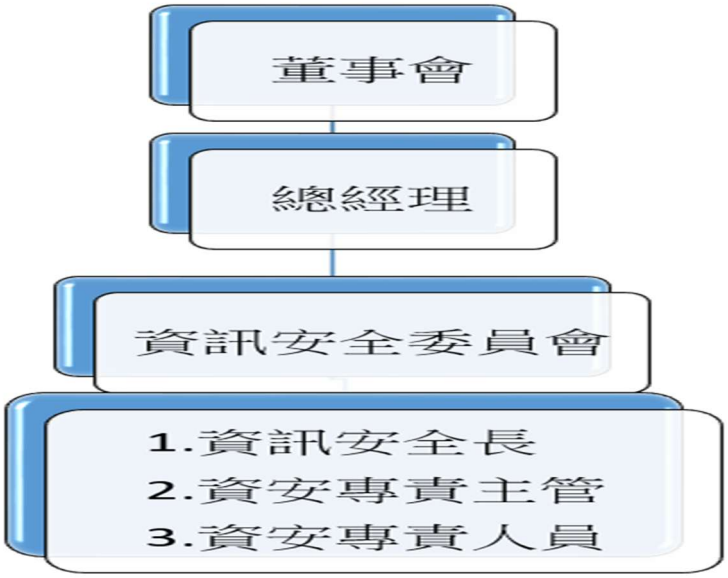
本公司之企業資訊安全組織，目前由資訊安全委員會組織成員統籌資訊安全及保護相關政策制定、執行、風險管理與遵循落實，本公司稽核處並肩負稽核企業資訊安全之責。

(2)企業資訊安全組織架構

依法設置資通安全專責主管及人員五名，並以資安專責主管為召集人執行審查資安管理政策、擬訂資安管理架構及組織功能，定期檢視公司整體資安管理機制之發展、建置及執行結果。其運作情形如下：

A. 由總經理指派專責主管與人員。
B. 至少每年開會二次(114 年開會次數為 2 次)。
C. 本公司之資訊安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項:

- 資通安全政策及目標之研議。
- 傳達公司資通安全政策與目標。
- 其他資通安全事項之規劃。
- 資通安全相關規章與程序、制度之執行。
- 資訊盤點及風險評估。
- 資料安全防護事項之執行。
- 資通安全事件之通報及應變機制之執行。
- 其他資通安全事項之辦理與推動。



2.資通安全政策

(1)資訊安全政策目的

確保本公司所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

(2)資訊安全政策原則

- 應考量相關法律規章及營運要求，進行資訊資產之資訊風險評估，確定資訊作業安全需求，建立「資訊安全管理辦法」作業標準，採取適當資訊安全措施，確保資訊資產安全。
- 依人員角色及職能為基礎，建立評估或考核制度，並視實際需要辦理資訊安全教育訓練及宣導活動。
- 資訊資產存取權限之賦予，應依業務需求並考量最小權限、權責區隔及獨立性審查。
- 建立資訊安全事件管理辦法，以確保事故妥善回應、控制與處理，訂定業務持續計畫並定期演練，以確保資訊系統或服務持續運作。
- 依據個人資料保護法與智慧財產權法之相關規定，審慎處理及保護個人資訊與智慧財產權。
- 定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實。
- 違反本政策與資訊安全相關規範，依相關法規或人事規定辦理。
- 為確保所有同仁知悉本身在資訊安全上應盡職責，應透過資訊安全持續訓練，強化同仁對資訊安全要求之認知。

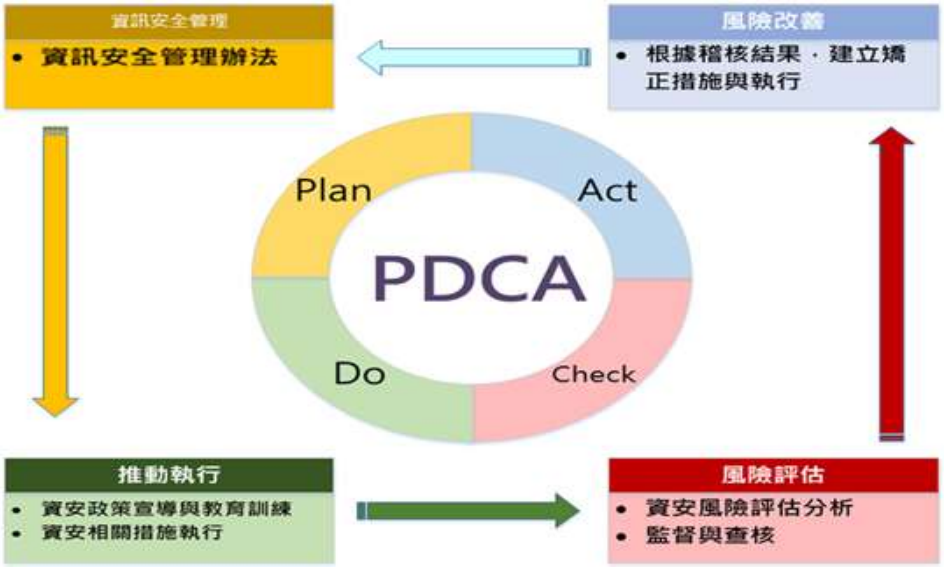
(3)資訊安全政策目標

- 維護資訊之機密性、完整性與可用性，並保障個人資料隱私。
- 保護業務服務資訊，避免未經授權的存取、修改，確保其正確完整。
- 建立資訊營運持續計畫，以確保業務服務之持續運作。
- 業務服務執行須符合相關法令或法規之要求。
- 組織每年依上述目標訂定量化量測項目，填寫於「目標管控及量測表」與「資訊服務水準量測表」，依實際執行情形管控。

(4)資訊安全管理策略

- 本公司資訊安全之權責單位為資訊安全委員會組織成員，負責規劃內部資訊安全政策、執行資訊安全管理辦法與資安政策推動與落實。
- 本公司稽核處為資訊安全監理之查核單位，並依所排定行程進行查核作業，若有發現缺失或風險，即請受查單位進行檢討，並提出具體改善計劃及時程，定期追蹤改善進度，以降低資安風險與落實資訊安全政策。
- 本公司資訊安全運作模式採用 PDCA（Plan-Do-Check-Act）方式管理，確保目標達成且持續改善。

(5)資訊安全風險管理與持續改善架構



3.資通安全具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

(1)建構多層次資通安全防護體系

- 網路安全:

  本公司已建置縱深防護體系，整合防火牆、網頁應用程式防火牆（WAF）、入侵防禦系統（IPS）、垃圾郵件過濾及端點偵測與回應系統（EDR）等多層防護機制，並透過資安監控中心（SOC）即時監控內外部威脅及資料存取行為，持續強化整體資通安全防禦能力。

- 設備安全:

  各項設備作業系統均安裝防毒軟體並定期更新病毒碼，相關系統及應用程式依規定進行弱點修補與版本更新，以降低資安風險。

- 帳號安全:

  全體同仁之帳號及重要系統帳號均依權限控管原則進行管理，並落實密碼管理及存取控管機制，以防止未經授權之使用。

- 資料安全:

  本公司建置完整之資料庫備份機制，並將備份資料進行異地保管，以降低資料遺失風險；同時定期執行備份及復原演練，確保資訊系統正常運作與資料完整性，並符合預期之系統復原目標時間。

(2)建立全員資通安全意識，強化資安風險管理文化

- 不定期透過電子郵件向全體同仁發布資訊安全相關公告，以提升日常資安警覺。

- 每年定期辦理全體員工教育訓練，進行資訊安全宣導，深化資安觀念。
- 每年邀請專業資安講師至公司辦理資安教育講座，強化資安人員對資安風險之認知。
- 每年辦理一次電子郵件社交工程實務演練，以檢視並提升員工防範資安威脅之能力。

(3) 落實持續監控，精進資通安全管理

- 弱點掃瞄:透過專業弱點掃描工具，定期對主機及網站進行弱點檢測，並依掃描結果執行漏洞修補，以降低潛在資安風險。
- 滲透測試: 每年定期委託第三方資安專業廠商辦理滲透測試，模擬外部攻擊情境，檢視系統與網路防護機制之有效性，並依測試結果進行改善，以強化整體資通安全防護能力。
- 制度檢討與持續改善：
  定期檢討資訊安全政策與管理制度，並依內外部環境變化持續精進，以落實資通安全管理。

4. 投入資通安全管理之資源

(1)資訊安全規章及程序:

為落實資訊安全管理，本公司於民國 113 重新修訂「資訊安全管理辦法」作業細則完成，並據以執行資訊工作計畫，嚴格控管設備安全、網路使用與安全管理、帳號權限申請流程、內外部人員存取控制、系統開發及維護控管與資安事件通報等，以減少公司資訊安全風險。

(2)定期進行內外部稽核:

除了每年實施內部稽核與會計師稽核，本公司預計於 2026 年第一季導入 ISO 27001 資訊安全驗證，以精進資安管理制度運作。

(3)投入資通安全管理之資源與外部聯防機制:

本公司於民國 111 年加入 TWCERT/CC，透過資安情資共享與聯防機制，強化資通安全威脅預警及應變能力。

(4)落實資安檢測、人員訓練與演練作業:

本年度已完成資安弱點掃描四次、滲透測試一次、員工社交工程演練一次並對點擊員工進行教育訓練及測驗、完成全體員工一次資安教育訓練課程、四次資安公告發信與企業持續營運演練一次，以持續提升整體資通安全管理成效。

(5)資通安全事件管理:

本公司已訂定資通安全事件通報與處理程序，明確定義各類資通安全事件之分級標準與通報流程，並於事件發生時即時啟動應變機制；事件處理完成後，進行原因分析與改善檢討，必要時修訂相關控管措施，以預防類似事件再次發生，持續強化整體資通安全管理效能。

5.重大資通安全事件：

本公司最近年度，並無發生重大資通安全事件而遭受之損失。