資通安全管理：

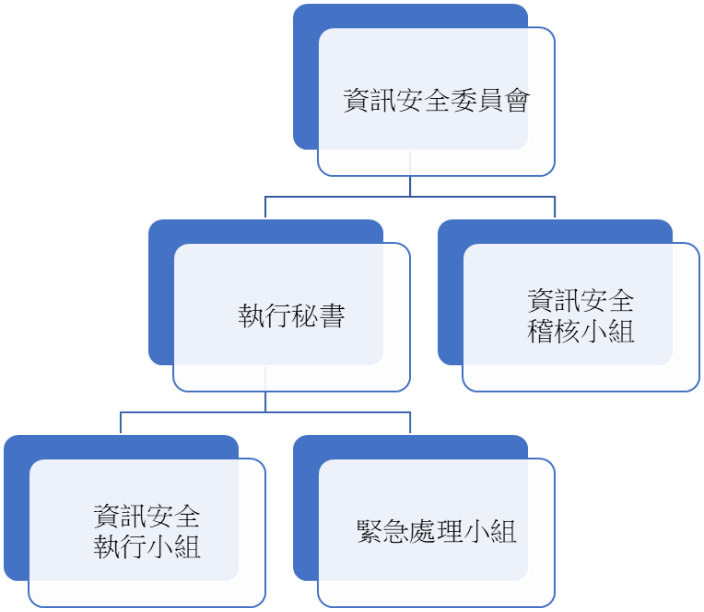
一、敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

(一)資通安全風險管理架構

1.企業資訊安全治理組織:

為落實本公司資訊安全，成立「資訊安全委員會」(簡稱資安委員會)任務組織，負責推動與統籌資訊安全管理系統之建置及維運事宜。

2.資訊安全組織架構:



3. 資訊安全委員會職掌:

(1)資訊安全委員會：為任務編組方式組成，由本公司資訊管理處處長擔任召集人，並由召集人指派委員，如因職務調動應即刻指派遞補人員與辦理交接。

(2)執行秘書：由召集人指派本公司資訊處經理擔任。

(3)資訊安全執行小組：為任務編組方式組成，由執行秘書指派人員擔任組長及組員，負責規劃及執行各項資訊安全作業。

(4)緊急處理小組：由本公司各關鍵業務流程負責人員組成。

(5)資訊安全稽核小組：由資訊安全委員會指派，負責評估資訊安全管理制度之執行情形。

4. 管理審查會議:

(1)資訊安全委員會每年應召開一次「管理審查會議」，必要時得召開臨時會議。

(二)資通安全政策

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供

本公司之資訊業務持續運作之資訊環境，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，特定此政策規範。

1. 願景與目標：
   （1）強化人員知能
   （2）避免資料外洩
   （3）落實日常維運
   （4）確保服務可用
2. 資訊安全目標：
   （1）辦理資訊安全教育訓練，推廣人員資訊安全之意識與強化其對相關責任之認知。
   （2）保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。
   （3）定期進行內部與外部稽核，確保相關作業皆能確實落實。
   （4）確保本公司關鍵業務系統維持一定水準的系統可用性。
3. 應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序辦理。
4. 資訊安全執行小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。
5. 審查：

   本政策應至少每年審查1次，以反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及資訊安全實務作業能力。

(三)具體管理方案

1、電腦設備安全管理

- 伺服器等主要設備均設置於專用機房，機房門禁採用感應刷卡進出，且保留進出紀錄存查。
- 電腦設備安裝端點防護軟體，病毒碼自動更新，確保能有效偵測病毒，強化惡意軟體行為偵測。
- 機台設備入廠上線前需經過掃毒程序，防止內含病毒或惡意軟體的機台進入廠內。

2、網路安全管理

- 連外網路設置防火牆控管、連外伺服器安裝端點防護及入侵偵測軟　體，偵測並阻擋外部入侵及攻擊行為。
- 內部網路設置攻擊行為偵測設備，及早偵測內部網路電腦異常感染行為，快速找出感染源。

3、存取權限控制

- 使用單位依所需之資訊功能、電腦應用系統及程式使用提出權限申請，並經單位主管及資訊單位主管根據其工作職責及系統授權表核准後，由系統管理者設定其使用權限。
- 重要文件資料限制權限存取及加密控管。
- 人員調職、離職時，資訊單位依異動資料適時修改或取消其帳號及使用權限，確保資訊安全。

4、系統的持續運作

- 機房主機配置不斷電與穩壓設備，並連結公司的發電機供電系統，防止停電或供電異常造成之系統損壞。
- 建置即時異地備援架構，當本地端機房因災害失去功能時，可由異地端備援主機及儲存設備啟動相關服務。
- 強化資料備份及復原機制，除每日排程進行儲存媒體備份外，亦啟用儲存裝置的定時 Snapshot(快照)功能備份，加強系統復原完整度及效率。

（四）投入資通安全管理之資源

本公司持續投入資源於資訊安全相關領域，在資通安全推動的主要成效下:

1. 113 年共實施三次無預警電子郵件社交工程演練與社交工程認知教育訓練，點擊信件連結比例低於 1%。
2. 每年協同母公司力成集團投保資安保險，預防事故造成重大財務損失，保障客戶及投資人權益。
3. 由廠商進行弱點掃瞄，針對掃描結果提出相關建議與掃描報告，並進行弱點修補作業，降低遭受入侵的風險。
4. 所有新進員工皆完成資訊安全教育訓練。
5. 公司於 114 年導入 ISO27001 並於 114 年 12 月通過 SGS 驗證。